

Biometric Fusion Demonstration System Scientific Report

Mcken Mak
International Biometric Group

Joseph Kim
International Biometric Group

Michael Thieme
International Biometric Group

International Biometric Group
One Battery Park Plaza
Ground Floor New York, NY 10004

Project Manager: S. Dahel 613-993-9949

Contract Number: W7714-030754

Contract Scientific Authority: Q. Xiao 613-998-1245

DEFENCE R&D CANADA - OTTAWA

Contractor Report

DRDC Ottawa CR 2004-056

March 2004

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE MAR 2004		2. REPORT TYPE		3. DATES COVERED -	
4. TITLE AND SUBTITLE Biometric Fusion Demonstration System Scientific Report				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defence R&D Canada -Ottawa,3701 Carling Ave,Ottawa Ontario,CA,K1A 0Z4				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT DRDC-Ottawa contracted International Biometric Group (IBG) to develop a biometric fusion application, utilizing three distinct fingerprint systems and one voice verification system. This application enables biometric data collection and sample matching as well as operator configuration of multi-system matching logic. The application provides sufficient data for DRDC to perform a range of quantitative analysis on the utility of biometric systems that use multiple systems within a given modality and multiple systems within multiple modalities. This document provides background information on the biometric technologies implemented within this demonstration application (fingerprint and voice verification). It describes various multimodal biometric concepts of operation for both verification and identification systems. It details the functionality accessible through the biometric fusions application. Lastly it provides an Operator manual for the application.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 75	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Approved by

Dr. M. McIntyre
Head/Network Information OperationsSection

Approved for release by

Dr. A. Ashley
Chief Scientist

The scientific or technical validity of this Contractor Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Terms of release: This document contains proprietary information. It is provided to the recipient on the understanding that proprietary and patent rights will be respected.

Abstract

DRDC-Ottawa contracted International Biometric Group (IBG) to develop a biometric fusion application, utilizing three distinct fingerprint systems and one voice verification system. This application enables biometric data collection and sample matching as well as operator configuration of multi-system matching logic. The application provides sufficient data for DRDC to perform a range of quantitative analysis on the utility of biometric systems that use multiple systems within a given modality and multiple systems within multiple modalities.

This document provides background information on the biometric technologies implemented within this demonstration application (fingerprint and voice verification). It describes various multimodal biometric concepts of operation for both verification and identification systems. It details the functionality accessible through the biometric fusions application. Lastly it provides an Operator manual for the application.

This page intentionally left blank.

Executive summary

Biometric systems are utilized to verify claimed identities, typically for access control, and to determine non-claimed identities, typically for identification of hostile parties. Different biometric modalities, such as fingerprint and facial recognition, are useful in different applications. However no single biometric system or modality provides optimal performance for all users in all environments. Multiple systems from within the same modality, or multiple systems from within different modalities, may be required to achieve desired performance. This is particularly true for military applications in which operating conditions may be much more challenging than the typical biometric usage environment.

IBG has designed an application through which DRDC can evaluate the utility of multi-system and multi-modal biometrics. Three fingerprint (silicon and optical) and one voice solution have been integrated into this application, while unlimited additional systems and modalities can be added. This application provides DRDC with an innovative method of configuring multi-biometric solutions in order to evaluate accuracy. Unique aspect of this approach include normalization of system-specific matching scores, allowing disparate outputs to be analyzed across a standard scale; availability of operator-configurable system logic, including combinatory and weighted, to enable detailed analysis of multi-system and multi-modal biometrics; and operator-triggered data capture functions, allowing acquisition of low-quality data as might be present in field applications.

Through this application, DRDC will be better able to specify, design, and implement biometric solutions that fully support its warfighters as they access and operate machines, equipment, materials, and communications devices. The potential benefits of multi-biometric solutions extend to both physical access to controlled areas and logical access to sensitive data. Different combinations of multi-biometric solutions can be assessed for initial identification and verification as well as periodic verification. Systemic combinations of sensors, algorithms, and modalities may be tuned for optimal authentication of individuals of differing ages, ethnicities, and physiology, such that a single multi-biometric system could address a population's divergent requirements. Lastly, identification of hostile parties may be effected through use of multiple technologies such as voice verification and facial recognition, searching watchlist databases comprised of full or partial facial images or voice recordings. Multiple-biometric systems can limit reliance on one input signal and allow for fusion of multiple inputs to narrow open searches.

These developments taken as a whole may have a substantial impact of the direction of military personnel and hostile authentication and identification, as the limitations of any one modality and/or sensor type are a major impediment to the widespread adoption of biometrics in challenging environments. However, fusion solutions such as those enabled through the delivered application greatly increase the viability of robust authentication.

Kim, J., Mak, M., Thieme, M. 2004. Biometric Fusion Demonstration System Scientific Report. [Enter report no.] International Biometric Group.

Table of contents

Abstract.....	i
Executive summary	iii
Table of contents	iv
List of figures	vii
1. Biometric Modalities Used in Fusion Application	1
1.1 Fingerprint Verification.....	1
1.1.1 Overview	1
1.1.2 Typical Applications	1
1.1.3 Landscape of Marketplace.....	2
1.1.4 Growth Drivers and Enablers	2
1.1.5 Growth Inhibitors	3
1.1.6 Competing Fingerprint Technologies.....	5
1.1.7 Trends in the Fingerprint Market: 2004-2008	7
1.2 Voice Verification	8
1.2.1 Introduction	8
1.2.2 Landscape of Marketplace.....	8
1.2.3 Growth Drivers and Enablers	9
1.2.4 Growth Inhibitors	10
1.2.5 Trends in the Voice Verification Market: 2003-2008	11
2. Multimodal Biometric Systems Overview	12
2.1 Situating Multimodal Biometrics in Biometric Applications.....	12
2.1.1 Application Functionality	12
2.1.2 Matching Functionality	13
2.1.3 Application Type	14
2.2 Multimodal Technology Combinations.....	16
2.2.1 Identification (1:N) Technology Ratings and Combination Assessments.....	17
2.2.1.1 Fingerprint and Facial Recognition	17

2.2.1.2	Iris Recognition and Facial Recognition.....	18
2.2.1.3	Fingerprint and Iris Recognition.....	18
2.2.2	Transactional (1:1) Technology Ratings and Combination Assessments.....	19
3.	Modeling Multimodal Systems	21
4.	Biometric Fusion Demonstration System (BFDS)	29
4.1	System Design.....	29
4.1.1	BFDS Design Concepts.....	29
4.1.2	Methodology for Choosing Technology Vendors	30
4.1.3	Challenges to Implementing Design Requirements	30
4.2	BFDS Development Software and Hardware.....	33
4.3	BFDS Applications.....	34
4.3.1	DRDC Enrolment	34
4.3.2	Cross Comparison	36
5.	Potential Enhancements to Military Applications	38
5.1	General Advantages of Multimodal Biometric Systems	38
5.2	Multimodal Biometrics in Military Applications	39
5.3	Challenges Facing Multimodal Systems	41
6.	Recommendations for Future Work	43
6.1	Technological Recommendations	43
6.2	Strategic Recommendations	43
Annex A:	BFDS Operator Manual	45
	BFDS Login.....	45
	BFDS Applications.....	46
	DRDC Enrollment: Operator Interface Map	47
	Main Enrollment Screen.....	48
	Enroll New Users	49
	Review and Add to Existing Enrollments	50
	Adding biometric to existing subject.....	50
	Enrollment Configuration.....	51
	Fusion-Based Matching.....	52

Collecting Live Samples.....	54
Fusion Results and Experiment Mode.....	55
Fusion Configuration.....	57
Cross Comparison	58
Cross Comparison configuration.....	59
List of symbols/abbreviations/acronyms/initialisms	60
Glossary	61

List of figures

Figure 1. Perspectives on Multimodal Biometric Applications.....	16
Figure 2. 1:1 – Non-Contingent – Binary – 2 System Sample Model.....	22
Figure 3. 1:1 – Non-Contingent – Scored Outputs Sample Model.....	23
Figure 4. 1:1 – Non-Contingent – Binary – 3 System Sample Model.....	24
Figure 5. 1:1 – Non-Contingent – Weighted Score – X System Sample Model	25
Figure 6. 1:1 – Contingent – Binary Score – Dual System Sample Model	26
Figure 7. 1:N – Non-Contingent – Rank 1 – 2 System Sample Model	27
Figure 8. 1:N – Non-Contingent – Candidate List – 2 System Sample Model	28
Figure 9. Voice Verification Input Schematic.....	33
Figure 10. Sample Cross Comparison .CSV Output	37
Figure 11. Application Icons	45
Figure 13. Main Enrollment Screen	48
Figure 14. Capture Interface.....	49
Figure 15. Reviewing Previous Enrollments.....	50
Figure 16. Enrollment Configuration	51
Figure 17. Fusion-Based Matching Interface	52
Figure 18. Selecting Samples for Fusion Matching.....	53
Figure 19. Live Acquisition Interfaces: Fingerprint and Voice.....	54
Figure 20. Fusion Output Interface.....	55
Figure 21. Fusion Configuration Interface	57
Figure 22. Cross Comparison Interface.....	58
Figure 23. Cross Comparison Configuration.....	59

List of tables

Table 1. Fingerprint Strengths and Weaknesses.....	5
Table 2. Voice Verification Strengths and Weaknesses.....	10
Table 3. BFDS Development Toolkits and Software	33
Table 4. BFDS Hardware	34
Table 5. BFDS Filename Data Elements.....	35
Table 6. Field Descriptions for cross comparison output files	37
Table 7. Application Description.....	46

This page intentionally left blank.

1. Biometric Modalities Used in Fusion Application

1.1 Fingerprint Verification

1.1.1 Overview

Fingerprint technology is based on the ridges, valleys, ridge endings, loops, whorls, and other features found on the human fingerprint. With the exception of AFIS technology, fingerprint is the leading biometric technology in terms of revenue generation. The success of fingerprint technology to date is primarily attributable to the following factors:

Maturity relative to other biometrics. With the probable exception of hand geometry, whose applications are comparatively limited, fingerprint is the most stable and proven biometric for 1:1 operations. The conceptual basis for fingerprint matching is well-understood, and results in a relatively accurate biometric technology.

Competition. A number of strong companies are involved in each segment of the fingerprint market, including algorithm development, sensor development, peripheral and access control device manufacture, and fingerprint-based application software. This competition has lowered prices and improved the quality of fingerprint solutions.

Breadth of applications. Fingerprint technology can be deployed effectively, including PC/enterprise network security, access control/attendance, and Civil Identification. The breadth of applications for which fingerprint is suited is a function of the technology's form factor and ease of use.

1.1.2 Typical Applications

Fingerprint technology is used by hundreds of thousands of people daily to verify availability for public services, access networks and PCs, enter restricted areas, authorize transactions, and access devices or equipment. The breadth of usage is such that there is no prototypical fingerprint application.

Most fingerprint deployments are 1:1, providing verification of a claimed identity. The manner in which a user claims his or her identity is based primarily on the application, ranging from smart card presentation to Windows username entry. The technology can also be implemented in "one-to-few" deployments, wherein individuals are matched against modest databases of perhaps 10-100 users. By eliminating the identity claim, one-to-few applications offer greater convenience at the cost of slightly increased

security risk. Large-scale 1:N applications, in which a user is identified from a database of thousands or millions of enrollees, are classified as AFIS.

1.1.3 Landscape of Marketplace

Fierce competition in various segments of the fingerprint market has limited companies' ability to operate profitably. Including OEMs and application developers, over 200 companies operate in this market. Approximately half of these companies are core technology firms, those that manufacture or develop one or more components of a fingerprint system.

The fingerprint market also contains hardware manufacturers and systems developers who OEM fingerprint sensors or modules or integrate fingerprint sensors and modules into existing products. Targus, Toshiba, Dell, and Compaq are among the leading OEMs who relabel and resell full fingerprint solutions from core technology vendors such as AuthenTec, DigitalPersona, and Identix.

Many security hardware firms in the business of electronic locks and door controls offer fingerprint technology as an optional extension to existing systems, although their ability to effectively sell, deploy, and service biometric systems has not been proven.

1.1.4 Growth Drivers and Enablers

Fingerprint growth is driven and enabled by the following factors:

Mature matching algorithms enable accurate and reliable operation. The fingerprint has long been recognized as a highly distinctive identifier; methods of classifying, analyzing, and studying fingerprints have been utilized for decades. Biometric fingerprint technology builds on this body of knowledge; while approaches to matching algorithm development differ, the use of friction ridges is biometrics' closest approximation to an exact science. Mature algorithms allow better fingerprint solutions to limit false matches to one in tens of thousands of placements. False non-matches can be kept to less than 1% with effective training on certain devices. When mature matching algorithms are deployed in conjunction with quality sensor technologies, fingerprint technologies can be deployed in applications predicated on either security or convenience.

Ease of use. The intuitive nature of interaction with fingerprint devices is also a primary enabler of growth in the fingerprint industry. While many competing biometric technologies require more complex user-system interactions, fingerprint technology requires fairly simple and precise actions on the part of users during enrolment and authentication. While other biometrics require less effort, such as facial recognition and certain iris

recognition devices, interaction with these technologies can be imprecise, with little feedback inherent in the acquisition process to direct usage.

Being an innately distinctive feature with a long history of use in identification, fingerprint technology is unique in the industry. While other physiological characteristics are more distinctive than fingerprints (irises and retinas, for example), the technology capable of leveraging these characteristics in an automated fashion is much less mature.

Competition has improved products, reduced costs. Competition in the fingerprint market has ensured continual improvement in core technologies, most notably in sensors and devices. This competition has led to dramatic cost reductions in certain market segments, with sensors now regularly priced below \$10 and devices below \$50. These price reductions benefit firms such as OEMs interested in incorporating biometrics into their products or devices. However, these cost reductions have not led to dramatic growth in logical or physical access applications: the cost to deploy biometrics in the enterprise or for access control solutions is tangential to sensor costs.

Form factor, modes of operation enable deployment in range of environments Fingerprint technology can be deployed in a wider range of applications than any competing biometric, expanding the potential range of revenue opportunities for sensor, peripheral, algorithm, and application software developers. Fingerprint is clearly the dominant biometric technology in the desktop market, providing a reasonable balance between ease of use and accuracy. Implementations of middleware solutions in PC/enterprise network security applications also invariably leverage at least one type of fingerprint technology, often multiple types. Fingerprint is less dominant in other applications but still has substantial penetration.

Within access control, fingerprint's primary advantage is cost. While lacking certain strengths of iris recognition and hand geometry, fingerprint-based access control devices are substantially cheaper than those of competing biometrics, and device costs are an essential differentiating factor in this space. Fingerprint is also expected to capture a reasonable percentage of revenues in Civil Identification applications such as border management, though competition is present in the form of facial recognition and to a lesser degree iris recognition.

1.1.5 Growth Inhibitors

Though radical changes in the composition of the marketplace or an overall loss of confidence in the technology would need to occur to undermine fingerprint's position in the biometric industry, the technology does face growth inhibitors, some of which may prove substantial.

Risk of technology obsolescence. As opposed to technologies such as facial recognition and voice verification, which can leverage existing acquisition

devices, fingerprint's growth is contingent on the widespread incorporation of sensors in keyboards, peripherals, access control devices, and handheld devices. The ability to acquire fingerprints must be present wherever and whenever users are enrolled or authenticated. This issue is complicated by the fact that devices are not interoperable, and that upgrading or migrating to new technologies generally entails complete re-engineering and reenrolment of one's user base. Therefore decisions to implement fingerprint technology can be stalled for fear of technology obsolescence. This problem impacts fingerprint technology uniquely, as all other biometrics either use generic input devices (face, voice, signature) or are instantiated in a globally interoperable core technology (iris, hand).

Stigma of fingerprinting . The stigma attached to fingerprints – especially in the U.S., Canada, Europe, and Japan – may reduce institutions' willingness to deploy fingerprint technology. Privacy advocates fear that fingerprint data collected for a specific purpose may be used for forensic applications or used to facilitate tracking of a person's various activities. The fear of data misuse is particularly acute in large-scale Civil Identification projects such as national ID and border management applications. Regardless of the counterarguments provided by biometric vendors and the biometric community at large, the general public's association of fingerprint technology with criminal uses cannot be ignored.

Susceptibility to spoofing. Recent tests demonstrate the susceptibility of fingerprint devices to spoofing, or the use of artifacts and materials to enroll and verify in fingerprint systems. While this susceptibility to spoofing does not impact all fingerprint applications¹, the publicity resulting from these tests has led to some scepticism regarding the viability of fingerprint technology for high-risk or high-security applications. If the "liveness detection" issue is not resolved to deployer satisfaction, especially in public sector applications, fingerprint technology may be directly impacted.

Inability to enroll all users. Not all individuals are able to enroll in fingerprint systems, due to worn, damaged, or otherwise unreadable fingerprints. Testing has shown that certain ethnic groups and population subsegments – the elderly, manual laborers, and some Asian populations, in particular – are more difficult to enroll than others. The implication of high failure to enroll (FTE) rates is that some number of users must be authenticated by another method, be it another biometric, a password, or a token. In an enterprise, this may result in reduced security as well as the need to maintain dual authentication methods. In a customer-facing application, a customer willing to enroll in a fingerprint system may be unable to. While all biometrics require some sort of exception processing to deal with outliers (those unable to enroll), fingerprint is seen as particularly susceptible.

¹ See <http://www.biometricgroup.com/reports/public/reports/liveness.html>

Performance over time. A variety of factors can cause certain fingerprint systems to reject a high percentage of legitimate users, particularly when substantial time has elapsed. This leads to reduced confidence in the technology on the part of large-scale deployers. Although the fingerprint is a fairly stable physiological characteristic, IBG testing indicates that certain systems' false non-match rates increase from 0% to 25% within a span of six weeks; at the same time, other fingerprint systems' performance remained unchanged. This tendency is especially problematic when dealing with a user base comprised of manual laborers. Ensuring a high-quality enrolment can improve long-term performance, while enrolling multiple fingerprints can also help to circumvent the problem.

Table 1. *Fingerprint Strengths and Weaknesses*

FINGERPRINT STRENGTHS	FINGERPRINT WEAKNESSES
<ul style="list-style-type: none"> • Accurate matching algorithms • Substantially improved acquisition technologies • Sensors can be built into various devices, form factors • Availability of multiple samples increases overall accuracy • More standardized than competing technologies • Strong competition in market drives technology development 	<ul style="list-style-type: none"> • Fingerprint quality varies by age, race; subject to wear and tear • Small percentage of users unable to enroll • Accuracy of certain solutions diminishes over time • Susceptible to spoofing • Sensor surfaces can be scratched • Association with forensic usage raises privacy concerns

1.1.6 Competing Fingerprint Technologies

Optical and silicon technologies are the most commonly deployed fingerprint acquisition technologies, while ultrasonic technology shows considerable promise for certain types of applications².

Optical

Optical technology remains the most widely used fingerprint technology, but by a much smaller margin than was the case prior to 2003. Optical technology utilizes coated, clear sensors or platens, built of hardened plastic or glass. A chip-based CCD or CMOS camera registers the image of the fingerprint against the platen; ridges appear as grey lines against a white background.

² Emerging solutions based on polymers, pressure, and fiber optics have gained very little market share.

Extraction and image optimization algorithms – residing on a module attached to the sensor, on a board within the device, on a local PC, or on a central server – process the image, gauge its suitability for template generation, locate distinctive features, and generate enrolment and match templates.

Optical technology has several strengths: proven reliability over time, resistance to electrostatic discharge, resolution of 500 dots per inch or more, and rapid image acquisition. Weaknesses include size constraints (optical devices are normally larger, heavier, and draw more power than silicon sensors) and susceptibility to spoofing.

Optical devices are deployed in PC/enterprise network security, access control/attendance, and Civil Identification applications. Optical technology is far and away the most widely deployed technology in programs that require large-scale enrolment of employees or citizens, such as the US DoD DEERS/RAPIDS program (which uses Identix optical technology). Silicon is less proven under challenging, heavy-usage conditions. This bodes well for optical technology's inclusion in border management programs such as US VISIT in which hundreds of thousands of individuals may interact with devices on a daily basis.

Silicon

Silicon technology has gained considerable acceptance since its commercialization in 1998; silicon has taken major steps to close the gap traditionally held by optical technology. The presence of STMicroelectronics, Infineon, Sony, and Fujitsu in this market, as well as the emergence of AuthenTec as a dominant technology provider, should continue to drive silicon's market share in the fingerprint space.

As opposed to optical technology's use of a plastic or glass platen, silicon technology uses an integrated circuit (IC) as a sensor. Most silicon fingerprint technology is based on capacitance, wherein the silicon sensor acts as one plate of a capacitor and the finger acts as the second plate. The capacitance between platen and finger is converted into a digital signal. A variation of silicon technology measures capacitance beneath the first layer of skin, such that the signal represents the live epidermal layer. Other variations measure heat and light emissions.

Silicon technology's strengths include image quality approaching that of many optical devices, modest size and depth requirements (such that sensors can be integrated into small, low-power devices), and ease of production, which contributes to reduce per-chip costs. Silicon technology's weaknesses include questionable durability, susceptibility to electrostatic damage, and performance in heavy-usage or otherwise challenging conditions.

Silicon sensors are almost invariably smaller than optical sensors, which is beneficial in certain usage scenarios and market segments but a disadvantage in others. Silicon devices are primarily deployed in peripherals for PC/enterprise network security or for device access (particularly laptops and PDAs). Silicon sensors have also seen increased uptake in access control/attendance applications. The technology is rarely if ever deployed in public sector verification applications, most likely due to (1) questions regarding robustness, (2) integrators' greater comfort with optical technology, and (3) a need to acquire a larger fingerprint area in applications with non-acclimated users.

Matching algorithms

The fingerprint industry is also divided into vendors that utilize minutia algorithms and those that utilize pattern-based algorithms. Minutia-based algorithms generate and compare templates based on the x , y , and θ of dozens of ridge endings and bifurcations found in fingerprints. Pattern matching algorithms are based on the regional characteristic present across multiple ridges as opposed to single points.

Approximately 65% of fielded fingerprint solutions use minutia-based extraction algorithms. However, pattern-based solutions – historically viewed as less proven than minutiae-based solutions – have gained traction for two reasons: (1) the advent of very small sensors that do not acquire sufficient fingerprint data to reliably utilize minutia and (2) the maturation of national and international standards that codify interoperable methods of pattern utilization.

1.1.7 Trends in the Fingerprint Market: 2004-2008

The fingerprint market will be increasingly divided between technologies optimized for small-form factor devices such as PDAs and peripherals and those optimized for Civil Identification and high-traffic applications. The former is driven largely by reductions in cost and power consumption; the latter is driven by large-surface sensors and reliability, measured as mean time between failure (MTBF).

Standards for image capture will provide a basis for vendors to use when acquiring images for storage, particularly in public sector systems. More importantly, template standards – developed separately for minutiae and for pattern-based technologies – will be adopted at the US and international levels, such that vendors can implement extraction and matching technologies that are interoperable across devices. Note that interoperability will still not be possible between pattern and minutiae, only within pattern and minutiae.

Both silicon and optical firms will develop swipe sensors of various form factors in order to respond to perceived market demand for low-profile

sensors. The effectiveness and usability of these solutions remains to be determined, and will be subject to testing and evaluation.

A larger percentage of revenues will be attributable to service offerings that leverage fingerprint functionality on a transactional basis. BioPay's service is the best example of this offering, although companies with broader capabilities and presence in the retail space – such as Hypercom or VeriFone – are better positioned to implement and draw revenues from fingerprint technology in the retail/POS space.

More independent software vendors will incorporate fingerprint technology within their applications in order to provide stronger authentication. This trend will manifest itself in health care, workflow management, HR, and other enterprise areas in which custom applications dominate the market. As a result the fingerprint market will become increasingly software-oriented, as applications are developed which leverage existing devices.

More fingerprint deployments will take place in multimodal applications in conjunction with technologies such as facial recognition. This approach is designed to more effectively address outliers – those unable to enroll in fingerprint systems.

1.2 Voice Verification

1.2.1 Introduction

Voice verification technology is based on distinctive characteristics derived from spoken phrases. These characteristics are determined by the physiology of the vocal tract and by the behavioural aspects of speaking. Voice verification is a strong solution for implementations in which vocal interaction is already present. It is not a strong solution when speech is introduced as a new process. Telephony is the primary growth area for voice verification, and will be by far the most common area of implementation for the technology. The largest opportunities are in financial services account access; other leading applications include customer authentication for service calls and challenge-response implementations for house arrest and probation-related authentication. These solutions often combine voice verification with speech recognition, such that spoken account numbers are used to both retrieve personal data and verify identity.

1.2.2 Landscape of Marketplace

Approximately 20 companies compete in the voice verification market, many of whom offer voice verification as one of many voice- and speech-related solutions. A handful of established companies dominate this market segment,

but voice verification revenues have remained modest. Solutions offered in this segment include the following:

- Core voice verification extraction and matching technology
- Custom integrated hardware and software solutions
- Packaged software solutions

It is very likely that larger companies will enter this market space as a complement to their existing work in speech recognition. IBM, for example, has announced its plans to roll out products across a range of voice applications, including biometrics. This type of development is likely to alter the landscape of the voice verification market.

1.2.3 Growth Drivers and Enablers

Voice verification growth is driven and enabled by the following factors:

Existing acquisition infrastructure . The strongest growth enabler of voice verification technology is the availability of telephones (both landline and mobile) as an acquisition infrastructure. As opposed to other biometrics, such as Fingerprint and iris recognition, whose growth is contingent on the distribution of proprietary acquisition devices, everyone with a telephone is a potential voice verification user.

Existing processes. Similarly, the ability to leverage existing processes is a critical voice verification growth driver. An end user can be enrolled in a voice verification system without a dedicated enrolment process, using spoken account numbers or personal data to generate an enrolment template. Verification is similarly transparent, with voice verification used in conjunction with an existing process.

Call centre cost reduction. The desire to reduce call centre costs by automating account access functions will be a primary driver of voice verification growth. Voice verification is used in conjunction with speech recognition products to ensure (1) that the proper account is retrieved and (2) that an authorized individual is accessing that account. As with all behavioural biometrics, voice verification can be used in conjunction with a “secret” value, such as the last four digits of a social security number. An impostor would need to know the answer to a challenge-response sequence and then be capable of defeating the biometric system. Even a moderately accurate voice verification solution capable of biometrically authenticating 80% - 90% of users, while routing 10% - 20% of callers through standard authentication processes, can significantly reduce call centre costs and ensure that operator screening efforts are directed at the most suspect callers.

The expansion of telephony-based services will also drive revenues, as consumers look for more granular access to information and transactions from land and mobile devices. Institutions need to strike a balance between securing personal information and providing access to information. Voice verification can provide an extra level of security, enabling expanded services with increased security.

The growth of speech recognition, a much more widely adopted solution than voice verification, will open markets to voice-based authentication. There are a number of applications in which “what is spoken” is made more important with certainty that the correct person is speaking. Currently many of the leading voice verification solutions are developed by speech recognition companies; synergies between these two industries will drive revenue growth.

Table 2. Voice Verification Strengths and Weaknesses

VOICE VERIFICATION STRENGTHS	VOICE VERIFICATION WEAKNESSES
<ul style="list-style-type: none"> • Leverages existing telephony infrastructure • Requires little training or effort • Certain solutions have very low false match rate • Pass phrase can be changed – an advantage of behavioural biometrics 	<ul style="list-style-type: none"> • Accuracy can be affected by illness • Reduced performance with mobile phones • Changing modes of enrolment and verification impacts accuracy • Not a strong desktop solution • Average user lacks confidence in technology

1.2.4 Growth Inhibitors

Voice verification growth may be inhibited by the following factors:

Need for further deployment to substantiate implementation . Voice verification solutions have not been widely deployed in real-world applications, such that potential deployers may not be convinced of the technology’s accuracy and scalability. Deployers will be hesitant to utilize voice verification in large-scale production environments without strong reference implementations. Because of this, expansion to very large-scale deployments will be incremental.

Accuracy requirements and scepticism. Voice verification technology must provide an adequate level of accuracy to ensure that both institutions and customers have confidence in the system. Although many voice verification solutions are highly resistant to false matching, systems can also be susceptible to false non-matching due to background noise, telephone quality,

or changes in a person's speech habits. Consumers will assume that voice verification systems do not allow impostors to access their account, but false non-match rates are more likely to be a problem. If voice verification cannot strike a suitable balance between security and convenience, both deployers and end users will express frustration with the system.

1.2.5 Trends in the Voice Verification Market: 2003-2008

PC-based voice verification will reach a small percentage of desktops, but only in applications where users are already accustomed to speaking to their computer. Voice verification will not reach large number of desktops independent of other voice-oriented applications; the act of speaking to a computer must become commonplace for voice verification to take hold in this environment.

An increased number of text-independent solutions will reach the marketplace, eliminating the requirement to recite a specific string of text. This is a much more challenging task than text-specific verification, but will enable interesting new uses of voice verification technology such as call monitoring.

Improved performance in challenging conditions and from device to device will expand voice verification's reach within mobile telephony. This will provide security for remote voice-based transactions, although Fingerprint companies are also targeting mobile devices as a suitable area for sensor deployment.

Voice verification logic will be built into mobile phone chipsets, allowing voice transmissions to be classified as trusted or non-trusted according to whether the speaker has verified successfully.

2. Multimodal Biometric Systems Overview

Multimodal biometric systems are those which utilize, or collect for the purpose of utilizing, more than one physiological or behavioural characteristic for enrolment, verification, and/or identification. Multimodal systems address specific problems found in monomodal biometric systems, including the following:

- Biometric systems are subject to false match and false non-match errors. Depending on the type of biometric system deployed, excessive matching errors can lead to security breaches, undetected fraud, and processing delays.
- Biometric systems are subject to failure to enroll and failure to acquire errors. Such errors can be attributable to lack of required physiological characteristics, to insufficiently distinctive biometric characteristics, or to an inability to adhere to device interaction requirements. Failure to Enroll (FTE) and Failure to Acquire (FTA) errors result in a percentage of individuals permanently or temporarily unable to use a given biometric system. This creates problems for deployers, as a backup authentication method must be maintained, and malicious users may intentionally fail to enroll in order to attack the weaker authentication method (e.g. password).
- Recent demonstrations have shown that many biometric systems can be fooled by non-live data, some with little effort, others with substantial effort. This raises the possibility that difficult-to-repudiate transactions could be created and associated with an individual without his awareness, and that individuals could easily circumvent 1:N detection through use of fraudulent data.

2.1 Situating Multimodal Biometrics in Biometric Applications

In determining which biometric applications and usage environments are best-suited for the introduction of multimodal solutions, biometric applications should be viewed the perspectives of *Application Functionality*, *Matching Functionality*, and *Application Type*. Each of these perspectives brings out different facets of multimodal solutions.

2.1.1 Application Functionality

As multimodal solutions emerge, a substantial percentage of deployments are likely to involve collection, storage, and archiving of multiple biometric characteristics without necessarily involving subsequent matching of these characteristics. Such multimodal data may be collected for future use, perhaps in systems external to that in which it was originally collected. The collection of data from Afghani detainees for use in watchlist applications is a good example of multimodal biometric data collection without a directly associated matching function.

Application Functionality captures the concept that multimodal biometric applications can be designed for both capture and storage of biometric data as well as for ongoing usage of biometric data. While most biometric systems are deployed for the purpose of ongoing authentication and/or 1:N functions (collectively viewed as matching), multimodal application functionality can be logically divided between enrolment-registration functions on the one hand and matching functions on the other.

This differentiation is important due to differences in concepts of operation across these two application categories. Many of the temporal, processing, and throughput constraints present at the point of matching in multimodal systems are not present at the point of enrolment-registration. Therefore a jurisdiction may decide to acquire multiple biometric technologies due to the relative ease of such acquisition – as well as in recognition of the one-time nature of most biometric enrolment events – for uses to be determined.

2.1.2 Matching Functionality

Matching Functionality in multimodal biometric systems is inclusive of duplicate enrolment detection, transactional authentication, and watchlist functionality. The benefits and challenges of multimodal solutions, and the viability of multimodal deployment, can vary depending on the type of matching being executed.

The collection of multiple biometric characteristics capable of conducting 1:N searches – fingerprints, irises, and/or facial images – is designed to facilitate subsequent matching functions with greater speed and accuracy. For example, a commonly proposed solution to the problem of the time and expense associated with large-scale AFIS searches involves the use of facial recognition to perform a very rapid initial 1:N search on a database. Such a search could return, for example, the top 25-30% of potential matches, and a more thorough search on the remainder could be executed through the more accurate AFIS technology.

The benefit of this approach is its ability to enable faster searches with less reliance on expensive centralized matching systems. Also, in this scenario, any individuals unable to enroll in an AFIS search could be searched through facial recognition as opposed to going completely undetected. Though facial recognition is certainly less accurate than AFIS, so long as the number of individuals searched using only facial recognition is kept relatively small, then match results could be evaluated manually.

The logistics of duplicate enrolment detection are also consistent with the use of multimodal biometrics. Biometric enrolment is generally a one-time process conducted at centralized locations under the supervision of an enrolment authority. Enrolment does not normally have extraordinary time constraints, as multiple processes (e.g. document verification) and pieces of information are being gathered during the process. Users must also be

instructed in how to correctly provide data. These factors provide an opportunity to acquire multiple pieces of biometric data without necessarily having a major impact on existing processes and transaction times.

A handful of complications are present in the use of multiple biometrics for duplicate enrolment detection. First, in order for a multiple-biometric duplicate enrolment solution to be highly effective, the initial search must generate very few, if any, false non-matches, or else a loophole for fraud is opened. Also, if an individual is unable to enroll in the first system, sufficient biometric data must be available to search the entire database with only one biometric. A deployer must be prepared to have access to only one of the two biometrics for duplicate enrolment detection.

Most of the same considerations involved in duplicate enrolment detection apply to watchlist systems, those in which a database of biometric records – potentially acquired under controlled conditions or acquired in the field – is searched to locate potential matches. One issue in watchlist applications that substantiates the collection of multiple biometrics on enrolment is the fact that watchlists may be comprised of multiple biometric types, and may be expanded over time to include new biometric types.

The third major category of multimodal deployment is transactional authentication, in which a claimed identity is validated or in which a single individual is located from a modest database. Transactional authentication applications include traditional physical and logical access applications. Transactional authentication is characterized, broadly speaking, by a need for limited transaction time and straightforward usage. The several types of transactional authentication systems, and their relation to multimodality, are addressed below.

2.1.3 Application Type

Multimodal biometric systems can be an effective solution in biometric applications whose concept of operations is consistent with the additional cost, user time and effort requirements, and/or processing requirements associated with multimodal biometric systems. Not all applications are ideal environments for multimodal solutions (although multimodal solutions have been developed for nearly every biometric application).

The following requirements inform whether multimodal biometrics are useful and viable for particular applications

Spoofing Mitigation Requirement. Applications in which there is reasonable risk of spoofing – or substituting non-live biometric data for the purpose of enrolment or authentication in biometric systems – are amenable to the introduction of multimodal biometric systems. Multimodal systems that require provision of more than one biometric sample, which includes all but select contingent multimodal systems, reduce spoofing risks. While viability

and risks of spoofing are normally tied to a technology (e.g. fingerprint) as opposed to an application, unattended applications are particularly susceptible to spoofing attempts.

Universal Enrolment Requirement. Applications in which an effort must be made to enroll a total user population, are well-suited to the introduction of multimodal biometric systems. Employee-oriented applications, such as physical access and PC/network security, are normally characterized by a need for such universal enrolment. Similarly, citizen-oriented applications such as entry-exit and welfare are characterized by a need for universal enrolment in order for the overall system to work effectively. Multimodal systems enable a deployer to approach (if not meet) universal enrolment requirements.

Accuracy/Integrity Requirement. Applications characterized by a high need for accuracy or records integrity are well-suited to the introduction of multimodal solutions. If configured correctly, with intelligent utilization of vendor-specific match scores and thresholds, multimodal solutions can provide greater security than most single biometric solutions, and can certainly limit overall FTE and FTA (which can contribute to reductions in security and database integrity).

Usage Environment Requirement. In order for a multimodal system to be implemented in a given application environment, the usage environment must be subjected to a viability check for the implementation of more than one biometric technology. Certain usage environments are ergonomic and logistical “fits” for more than one biometric; however, the extra size and manoeuvring area necessary for multimodal solutions can overwhelm other operating environments.

Transaction Time Requirement. Most multimodal technology combinations present user interface challenges that constrain usage in time-constrained applications. Conversely, applications in which time constraints do not heavily impact transactions are more amenable to the use of multimodal biometric systems.

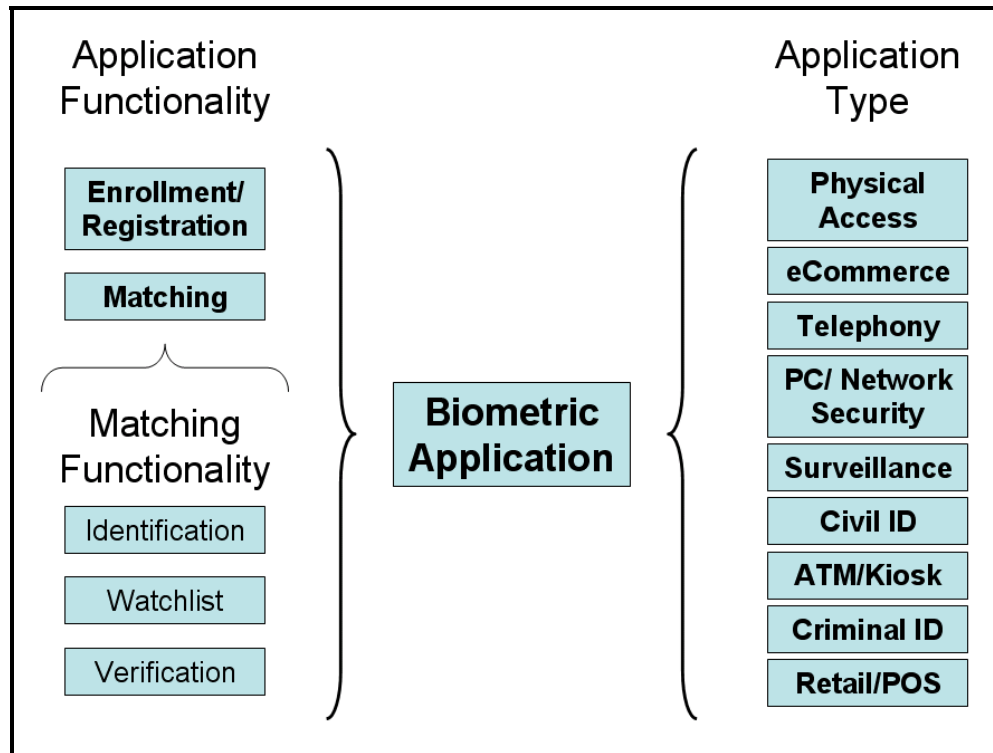


Figure 1. Perspectives on Multimodal Biometric Applications

2.2 Multimodal Technology Combinations

Since the late 1990's, biometric developers and systems integrators have developed systems capable of utilizing a wide range of biometric technologies in a rudimentary and/or multimodal fashion. The ability to enable several biometric technologies simultaneously demonstrates application-level flexibility, if not real-world usefulness. However, a rational approach to combining multiple biometric technologies must be implemented in order to ensure that technologies deployed are complementary and serve to minimize overall system weaknesses.

An ideal biometric would feature strong matching, require little effort, and be universally available and measurable. Modeling an ideal multimodal biometric requires that technology limitations be offset in each category by one or more complementary biometric technologies. The following are the four primary criteria necessary to evaluate technologies' suitability for multimodal biometric systems:

- Accuracy, or a technology's resistance to false matching and non-matching.
- Ease of Acquisition, or the level of effort required to provide enrolment/registration-level biometric data.

- Availability, or the presence of a biometric characteristic across a potential user base.
- Measurability, or the ability of a biometric characteristic to be reliably and accurately imaged in a field environment.

Suitable combinations differ for 1:N and 1:1 applications, whose characteristics vary fundamentally. An additional multimodal ratings criterion for 1:N applications, Legacy Database Compatibility, is included to capture the concept of backward-compatibility with existing data.

When determining what technology combinations are best suited to joint implementation, the less qualifiable element of acquisition synergy is also considered. Certain technology combinations may be capable of being acquired through devices with complementary interfaces.

2.2.1 Identification (1:N) Technology Ratings and Combination Assessments

2.2.1.1 *Fingerprint and Facial Recognition*

The use of fingerprint and facial recognition as a 1:N multimodal solution provides advantages in terms of ability to leverage legacy databases and (in the case of facial recognition) to leverage existing processes such as photo capture. Because facial recognition has been sanctioned by ICAO as the primary interoperable biometric technology for passport usage, it is likely that substantial effort will be dedicated to developing multimodal solutions that utilize this mandatory data piece in addition to more reliable identifiers such as fingerprint and iris recognition. In terms of 1:N functionality, facial recognition's ability to function as a gross classifier allows it to reduce the size of large 1:N databases and to effect more rapid 1:N fingerprint searches. Executing parallel full-scale 1:N searches through both fingerprint and facial recognition is unlikely to prove highly beneficial, as the results from the facial recognition will not be reliable, even on small databases. This underscores a challenge of this technology combination: if fingerprints cannot be obtained from a given subject, then only facial recognition can be utilized, meaning that a much less robust 1:N search would need to be executed. Furthermore, a deployer cannot simply assume that a search is required only on a database of individuals unable to enroll in the fingerprint system. A motivated individual can mar his or her fingerprints such that he or she could fail to enroll after having enrolled previously. Therefore facial recognition must be optimized to work as a standalone system to avoid providing

impostors with simple workarounds. Potential Solution For: Large-Scale Civil ID Systems; Criminal ID Systems.

2.2.1.2 *Iris Recognition and Facial Recognition*

Iris recognition and facial recognition bring the substantial advantage of being capable of being imaged through a single user process and through a single-housing acquisition device (which may contain two separate imaging elements). Therefore many of the process-driven impediments that face multimodal systems are not present in this technology combination. Narita Airport in Tokyo is testing this exact technology combination to determine the efficacy of the combined technologies. The limitation of this technology combination has to do with the relatively marginal role that facial recognition can play in a system with a strong and highly available biometric such as iris recognition. In most cases, if the iris can be reliably imaged, then the facial recognition components will add very little, such that the cost/benefit of collecting and maintaining such data can be called into question. Also, since iris recognition is always deployed as a day-forward solution as opposed to a solution that leveraged legacy data, there is less need to address existing large-scale databases. In extremely large-scale 1:N systems, facial recognition could serve as a gross classifier to reduce the demands on the 1:N iris search, as iris technology has not been deployed in highly scaled application environments (those with 1m+ enrollees). Potential Solution For: Large-Scale Civil ID Systems.

2.2.1.3 *Fingerprint and Iris Recognition*

For systems in which certainty regarding match results is an absolute necessity, fingerprint and iris recognition offer similar capabilities in terms of reliable 1:N matching. Fingerprint is more proven in real-world applications, and has been shown to scale with large loads of applicants; iris recognition is harder to circumvent than fingerprint technology, is more universally available, and provides high levels of accuracy. Each technology offers multiple samples, increasing scalability and accuracy. It is likely that for many deployers, iris recognition and fingerprint represent similar-enough capabilities that using both will be excessive. Neither is designed to provide the rapid, inexpensive database-reducing 1:N gross search functions of facial recognition. Potential Solution For: Large-Scale Civil ID Systems.

2.2.2 Transactional (1:1) Technology Ratings and Combination Assessments

Multimodal combinations for 1:1 applications will in most cases centre on use of fingerprint technology with a complementary biometric such as facial recognition or voice verification. Fingerprint technology has the advantage of being available in a range of form factors for PC/network access, physical access, retail, and other transactional applications. However, a small percentage of individuals are unable to enroll in fingerprint systems due to low-quality or nonexistent fingerprints. The use of multimodal biometrics is likely to take place in applications that are mandatory and entail enrolment of an entire population, such that a secondary biometric must be available. This suggests that both facial recognition and iris recognition, as above, are likely to be deployed in conjunction with fingerprint technology in certain environments.

A major variable in 1:1 multimodal systems for transactional authentication is whether facial recognition technology will continue to improve to the point where it can be used reliably in transactional environments. As the technology improves, it is a logical choice for multiple-biometric systems, because cameras can be deployed fairly easily and the process of providing facial images is not difficult. However, relatively few deployments currently use facial recognition for transactional authentication.

In certain cases the secondary 1:1 biometric may be made available for users who find the primary biometric objectionable or offensive. This decision must be approached cautiously, as a multimodal system can reasonably be viewed as being only as strong as the weakest single technology to which users have recourse. If, for example, users are given discretion to revert to facial recognition as opposed to fingerprint recognition simply because the fallback or secondary technology is present, then a major loophole is introduced in the system. Users motivated to circumvent the biometric system would simply avoid the strong biometric technology. This logic also impacts deployer procedures: there is a risk that a system operator will revert too quickly to a weaker fallback biometric should the stronger primary biometric fail, with the result that overall system robustness is reduced.

It is similarly likely that certain technologies will not gain substantial traction in the multimodal space, not due to any inherent limitation but simply due to the environments and applications for which they are suited. Signature-scan and voice verification technologies are often tied to a specific type of functionality, and are commonly implemented directly atop existing processes, such that incorporation of an additional biometric technology is inconsistent with the application's core operations. Hand geometry offers some potential for multimodal usage; one of the first proposed multimodal systems incorporated hand geometry and facial recognition for Israeli border control. One impediment to multimodal solutions using hand geometry is that hand geometry is often deployed as a deterrent in reasonably low-risk

environments – time and attendance, for example. There may not be sufficient motivation to incorporate new technologies for reduction or FMR or FNMR at the point of authentication.

3. Modeling Multimodal Systems

In order to fully understand the range of deployment options available to multimodal biometric deployers, and to logically map multimodal transactions, it is valuable to render a handful of multimodal deployment models through the steps of matching, output, logic, and decision. The following models can be used as a starting point for developing multimodal systems, ranging from 1:1 binary decisioning systems to weighted-rank identification systems.

Permutations of the following system models could easily run into the hundreds. The following samples are selected to demonstrate breadth of functionality as well as the changes resulting from slight alterations to multimodal concepts of operations.

Note that in the following models the acquisition and matching stages have been rolled into a single matching phase; it can be assumed that the number of acquisitions is equivalent to the number of match events. In addition, for certain models, Logic Processes are encapsulated within the output/decision phase for simplicity.

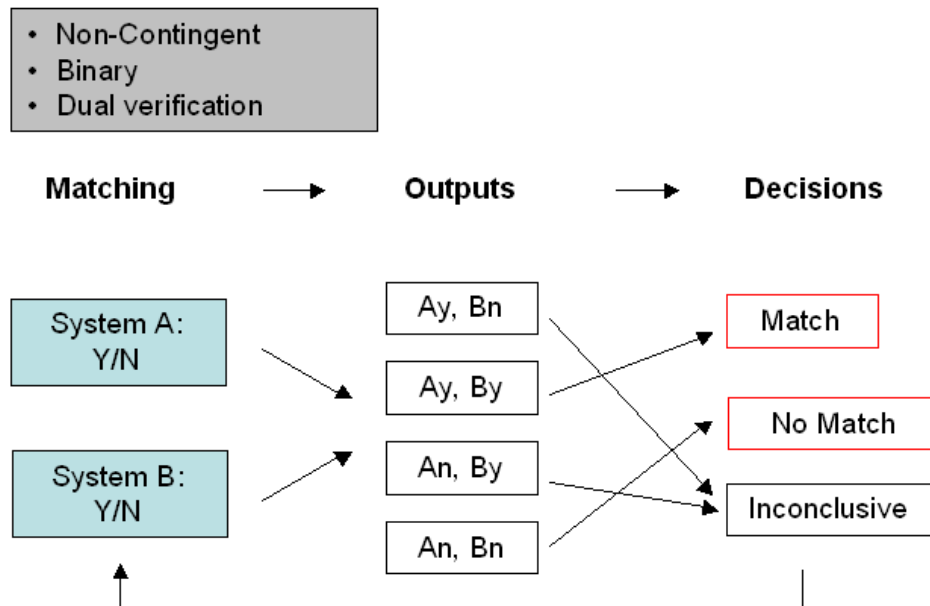


Figure 2. 1:1 – Non-Contingent – Binary – 2 System Sample Model

This model shows the simplest possible multimodal system: a two-biometric multimodal system with simple binary outputs and combinatory logic. Depending on deployer requirements, 1 successful match could be sufficient to render an overall “match” decision, may be a failed match, or may require an additional attempt. Though not indicated here, this re-authentication may be required through each system or only through the system in which the user was rejected. The lack of contingency at the matching fails entails acquisition of samples from each biometric system. Note that, for simplicity, the “logic” element is not rendered here due to the obvious use of and/or logic resulting from the output phase.

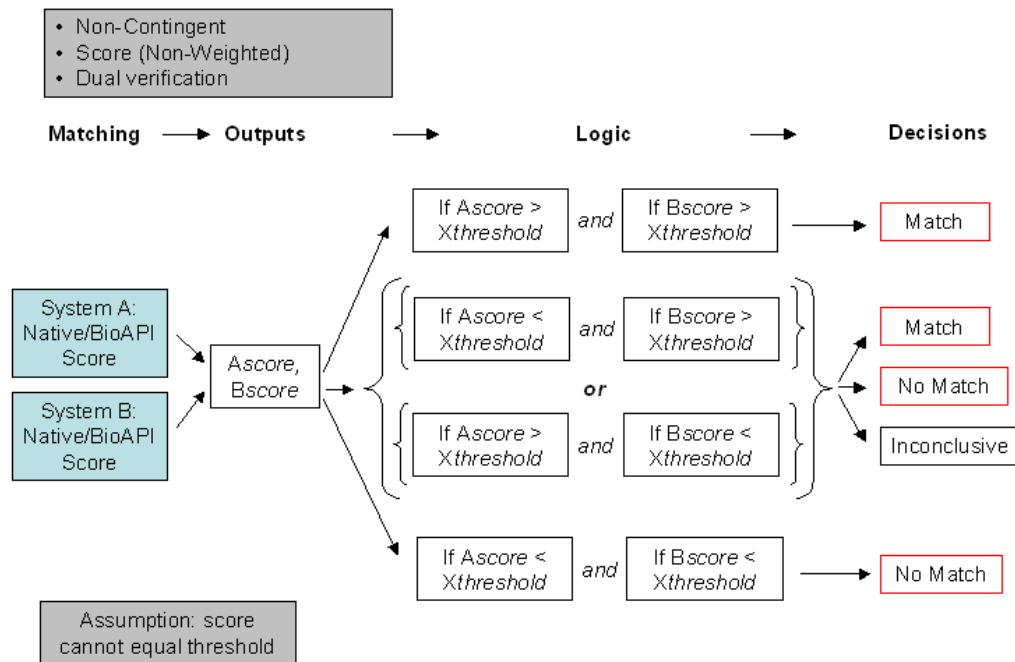


Figure 3. 1:1 – Non-Contingent – Scored Outputs Sample Model

This model shows the use of match scores to render an overall system match decision. In most cases multimodal systems require that a match output provide native or standardized match scores in order to give the granularity necessary to use multimodal logic. In this case the straightforward model is presented in which either zero, one, or two systems surpass the required match threshold. Deployer decision policy drives the determination whether one or two systems are required to declare a system match.

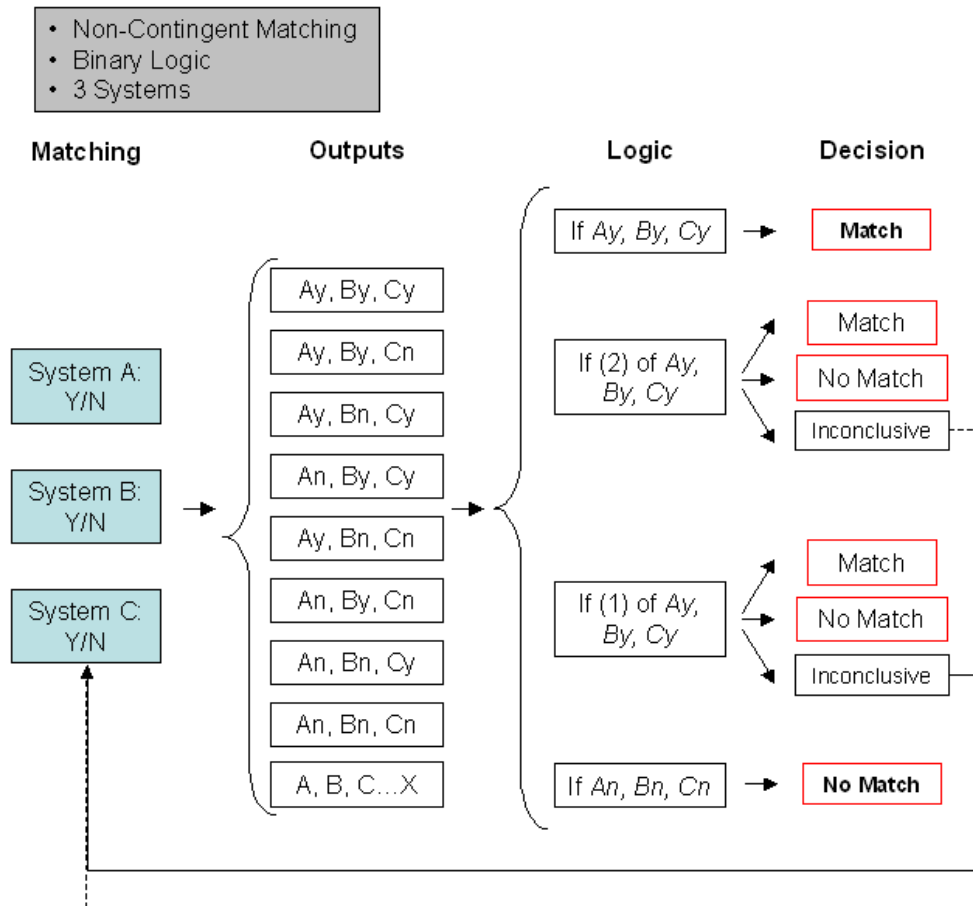


Figure 4. 1:1 – Non-Contingent – Binary – 3 System Sample Model

This model shows a three-biometric multimodal system with simple binary outputs and combinatory logic. Depending on deployer requirements, between 1 and 3 successful matches could be sufficient to render an overall “match” decision. Note that the lack of contingency at the matching fails entails acquisition of samples from three biometric systems. In most cases matches in 2 of 3 systems would be rendered an overall system match, while a match on only one system may be rendered inconclusive, such that re-authentication may be necessary. Though not indicated here, this re-authentication may be required through all systems or only through the systems in which the user was rejected.

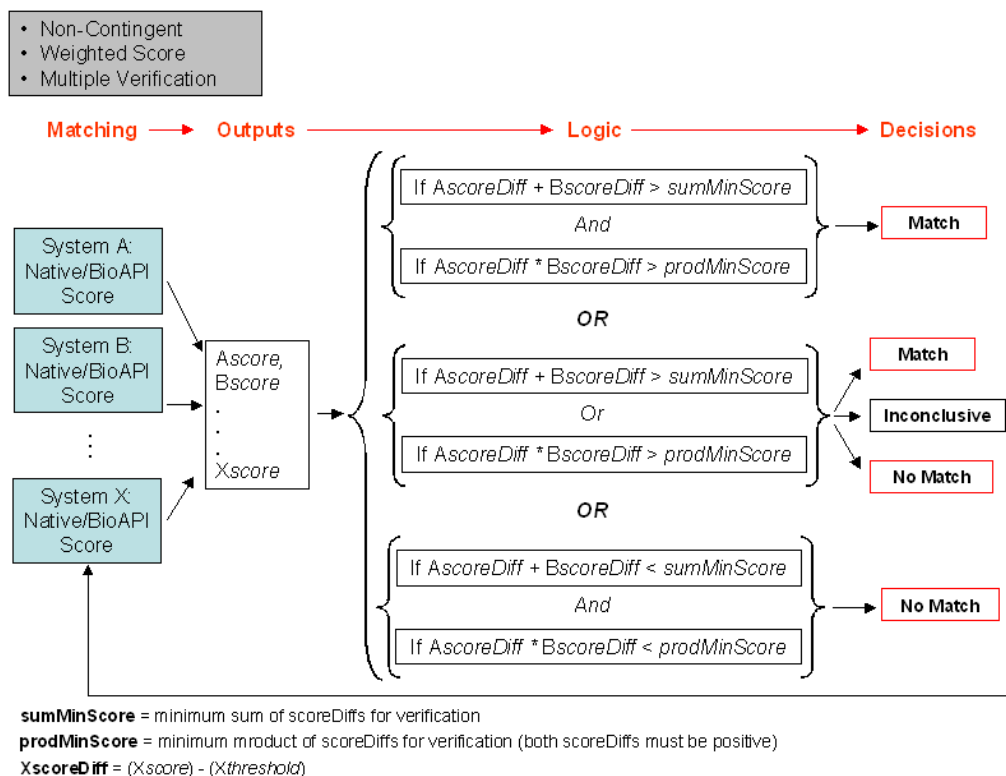


Figure 5. 1:1 – Non-Contingent – Weighted Score – X System Sample Model

This model shows the effect of weighted scoring on overall multimodal system operations. The concept of a very strong match being allowed to drive match decision to a greater degree than marginal match or non-match events is designed to reduce FNMR in operational systems, with the logic that a fielded system should not be subject to false matching at high levels of probability. Therefore the concept of a score differential (scoreDiff) is introduced that indicated the percentage, ratio, or raw count by which the actual match exceeds the required match level. In this model, score differentials can be summed (such that one score could actually fall under the required level but the sum exceeds the required match level) or made products (such that each system would need to exceed the minimum threshold to warrant inclusion). Clearly many more sophisticated variants of these models can be developed; the key concept is a weighted score differential to ensure that truly strong matches are given sufficient weight. Note that native scores are proprietary, while BioAPI scores fall on a 0-100 continuum, although the manner in which proprietary scores are mapped to BioAPI scored is proprietary.

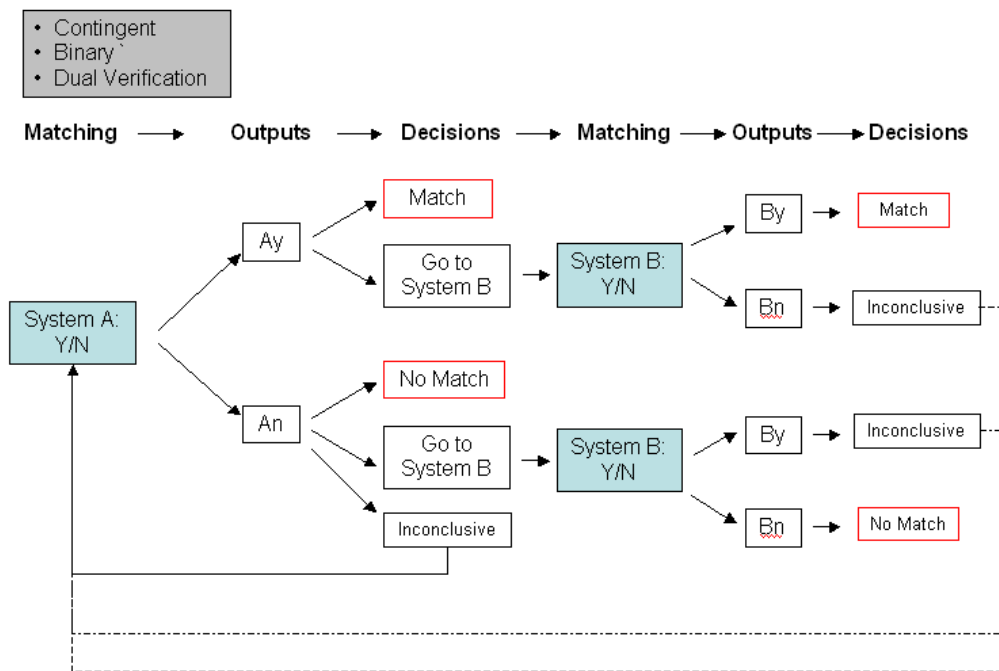


Figure 6. 1:1 – Contingent – Binary Score – Dual System Sample Model

This model shows the effect of contingency on multimodal system operations. A contingent system is a low-impact multimodal system designed not so much for the purpose of reducing FMR as for (1) reducing FNMR through fallback authentication and (2) reducing the impact of FTE by providing a secondary authentication method. As modeled above, acquisition through System B may be contingent on an unsuccessful match in System A or may always follow a successful System A match. System decisions may also require only one match or two matches.

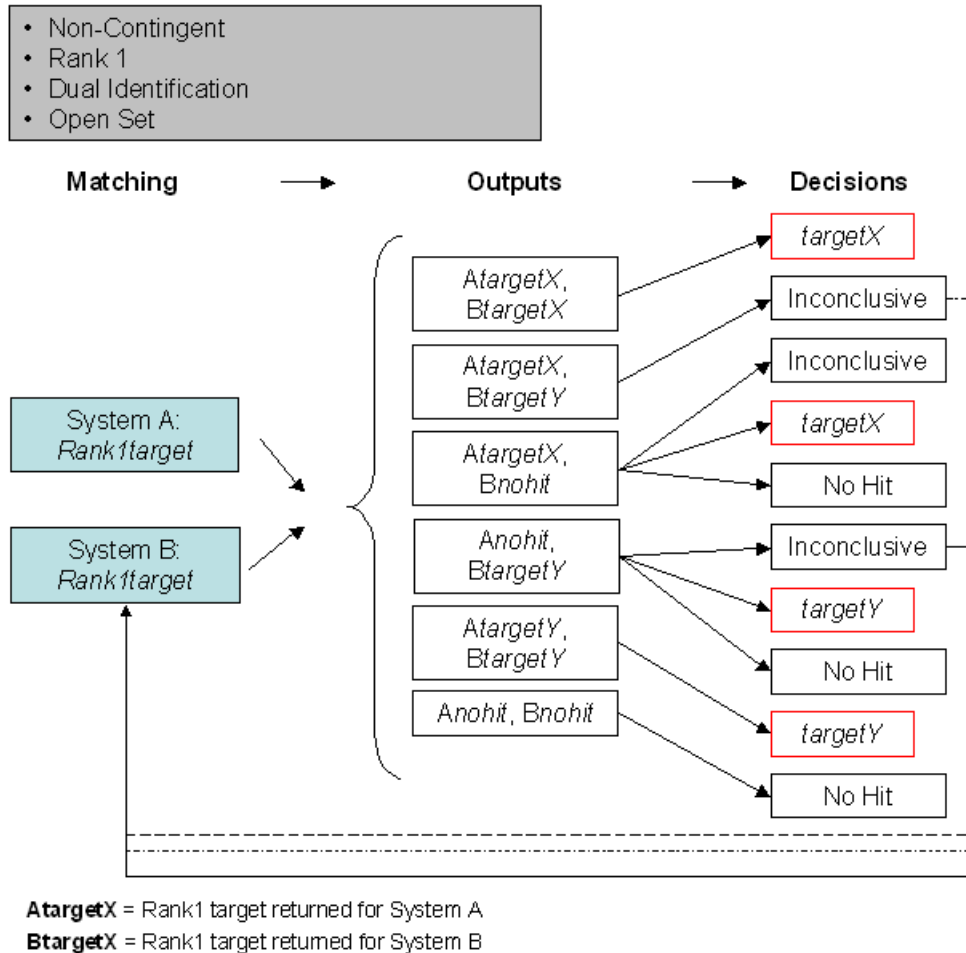


Figure 7. 1:N – Non-Contingent – Rank 1 – 2 System Sample Model

This model shows a two-biometric multimodal identification system utilizing Rank 1 and no-hit outputs and combinatory logic. Depending on deployer requirements, a single Rank 1 hit may be sufficient to result in a positive identification (perhaps triggering a manual image inspection), or two such Rank 1 hits may be necessary. In addition, the system may return two different individuals as Rank 1 hits, which in itself could trigger various resolution processes. The open set nature of this application indicates that the person being searched is not necessarily in the database, such that a “no hit” is a potentially valid system response if the person is indeed not present in the database. This is a contrast to closed set identification, in which the subject is known to be in the database and “no hit” is not a valid response. Note that, for simplicity, the “logic” element is not rendered here due to the obvious use of and/or logic resulting from the output phase.

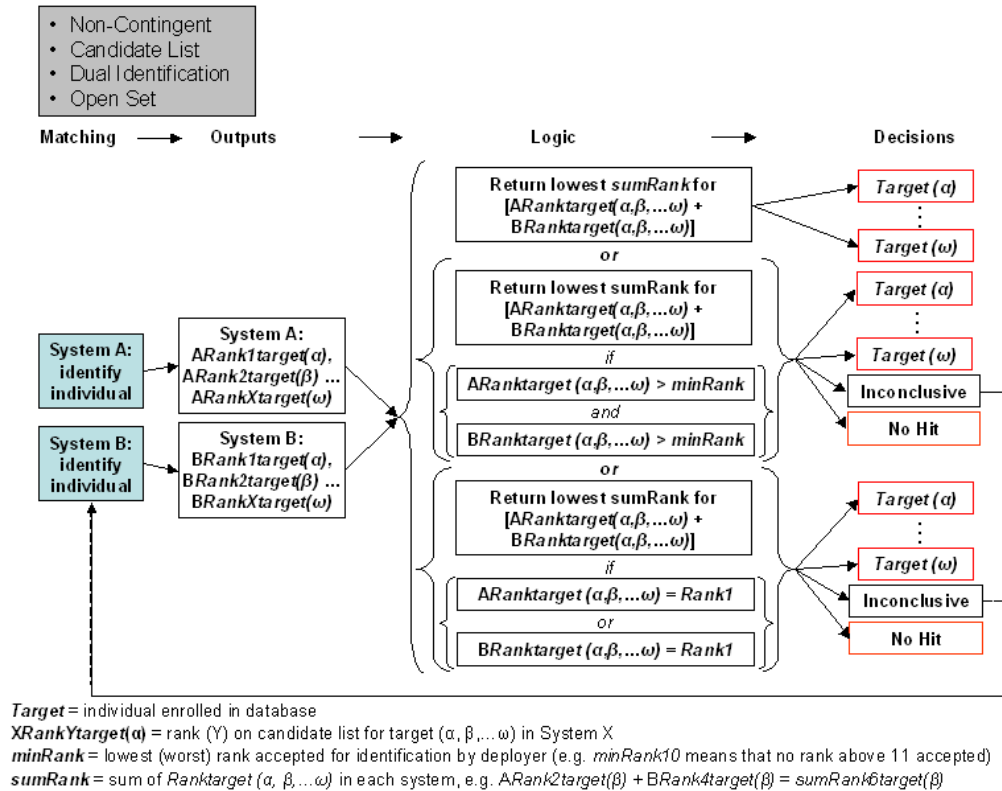


Figure 8. 1:N – Non-Contingent – Candidate List – 2 System Sample Model

This model shows a more complex variant of the preceding model utilizing two-biometric multimodal identification, candidate lists, and combinatory logic. This multimodal implementation is complicated by the fact that a range of individuals can be returned at various rank positions through different biometric systems. This figure renders different options available to the deployer in terms of decision policy. The logic can incorporate the lowest sum ranks across each system (e.g. Rank 2 on System A and Rank 4 on System B results in a sumRank 6); can incorporate a minimum Rank level (*minRank*) below which a match is not taken into consideration; or can mandate that a Rank 1 be a precondition of declaring a match.

4. Biometric Fusion Demonstration System (BFDS)

The Biometric Fusion Demonstration System is a custom-built application that enables biometric matching through multiple systems and modalities, presents vendor-specific scores resulting from such matching, and provides mechanisms for weighting and combining these scores to facilitate investigation of the degree to which fusion of scores from multiple systems and/or modalities can improve overall system accuracy. The system delivered to DRDC enables three fingerprint systems and one voice verification system.

4.1 System Design

4.1.1 BFDS Design Concepts

IBG designed BFDS with the flexibility to enable DRDC to efficiently collect data and perform customizable fusion score analysis. Since there are currently no commercially available systems that have the requisite modularity to facilitate these activities, especially with regard to image acquisition quality control and providing matching scores for authentication decisions, IBG built a customized demonstration system that would fulfill DRDC's requirements. BFDS was designed to perform the following functions:

- Perform data collection for DRDC to facilitate various analytical studies
- Generate matching scores from each system to enable DRDC to study and analyze different methods for fusing system-level results
- Demonstrate multi-model biometric matching and decision algorithms that can be customized and configured for testing several different fusion authentication methods

BFDS leverages the following design concepts in order to provide DRDC with the flexibility to fully explore issues in biometric fusion.

- Operator action is required during biometric acquisition in order to allow for manual control over the quality in input data and method by which such data is presented.
- The system provides operator feedback via a quality score to allow the operator to quickly review the quality of the acquired biometric sample (image and/or voiceprint).
- The system is capable of conducting cross-comparative matching, inclusive of data from both genuine users and impostors as well as from like- and non-like samples (e.g. index vs. middle fingerprints).

The system generates match results, including cross-comparative results, in a comma separated value (CSV) output file to allow DRDC to export this data to any application, database, statistical program (e.g., MATLAB) for further analysis.

4.1.2 Methodology for Choosing Technology Vendors

The systems integrated into the BFDS were as follows:

- Fingerprint System 1: Cross Match Sensor and SDK
- Fingerprint System 2: Sagem MORPHO Sensor and SDK
- Fingerprint System 3: STMicroelectronics Sensor, Bioscrypt SDK
- Voice Verification System: Nuance SDK, custom built signal acquisition and amplifier switch box

IBG considered several factors for selecting the three fingerprint verification vendors and the single voice authentication vendor.

- **Market presence.** Only top tier vendors active in the biometric industry for several years, and with significant deployments, device sales, and/or revenues, were considered viable candidates.
- **Previous benchmarking.** Vendors benchmarked by IBG through various rounds of Comparative Biometric Testing and other customized testing were seen as having demonstrated sufficient performance to warrant consideration.
- **Maturity of technology.** Candidates are representative of best-in-class technologies in their respective markets.

IBG ensured that both optical and silicon fingerprint capture technologies were represented: Sagem MORPHO and Cross Match provide optical technology, ST Microelectronics provides silicon. Note that Sagem MORPHO and Cross Match provided both fingerprint capture devices and matching algorithms, while ST Microelectronics' sensor was paired with a Bioscrypt specifically designed for use with this sensor.

4.1.3 Challenges to Implementing Design Requirements

Several challenges complicated BFDS design and execution, stemming from both interoperability issues as well as the unique scoring mechanisms of each technology. Innovative solutions were required to address the following challenges.

Inconsistent Application Programming Interfaces. While BioAPI is the most established biometric application programming interface, vendors SDKs were not compliant with this standard. Those vendors who provided a BioAPI interface did so in a variable fashion. To solve this problem, IBG created a plug-in for each system, as well as a plug-in manager used to discover and manage the plug-ins. This solution enables DRDC to develop its own plug-ins in order to add more devices and algorithms to the BFDS in the future.

Varying Range of Scores. The four systems generated biometric scores of different ranges and scales. IBG addressed this problem by normalizing the scores from each of the vendors to a fixed range from 0.0-100.0. “0.0” indicates the minimum match value, while “100.0” indicates the maximum match value. Systems’ scores were normalized on this scale as follows:

- **Nuance:** The vendor does not supply a fixed range for matching scores. Comparisons result in numerical scores, most often a single digit followed by several decimal point values (e.g. 2.338442; -3.440298). Based on internal testing and observation of system behaviour for genuine and impostor transactions, IBG selected [-5.0, +5.0] as Nuance’s score parameters. Scores outside this range are rendered as -5.0 or +5.0. Nuance scores are normalized to the global [0.0, 100.0] through the formula: [Normalized score = (Nuance score+5.0) * 10]. The vendor’s recommended passing threshold is zero, or 50.0 after normalization. One exception to the 0.0 – 100.0 normalized score range is when the system encounters a communications error: this results in a system-generated score of -100, well outside the range of normal match scores.
- **Cross Match:** The vendor’s score range is [0, 99]. Vendor provides whole numbers, not decimals. The formula for normalizing the scores was [Normalized Score = Cross Match score * (100.0 / 99)]. The vendor’s recommended passing threshold is 70, or 70.7 after normalization.
- **Bioscrypt:** The vendor’s raw score range is [0.0, 1.5]. Bioscrypt scores are normalized to the global [0.0, 100.0] through the formula: [Normalized score = (Bioscrypt score / 1.5) * 100.0]. The vendor’s recommended passing threshold is 0.4, or 26.667 after normalization.
- **Sagem MORPHO:** The vendor does not supply a fixed range for matching scores. Based on internal testing and observation of system behaviour for genuine and impostor transactions, IBG selected [1000, 25000] as Sagem MORPHO’s score parameters. Nuance scores are normalized to the global [0.0, 100.0] through the formula: [Normalized score = (Nuance score / 240) - (100.0 / 24)]. The vendor’s recommended passing threshold is 3000, or 8.3 after normalization.

While this normalization approach provides a baseline for assessing the viability of fusion approaches, it is not an absolute solution. As certain

vendors report non-fixed scores, IBG made the best estimation for the most probable score ranges in creating the normalization formulae.

Modularity in Fusion Decision Methodology. The demonstration system required a highly flexible design to showcase the different kinds of fusion method. This is a unique requirement, as most real-world implementations of multimodal systems would have a single, static fusion method for a particular application. IBG designed two fusion methods to generate multi-system weighted decisions.

- **Binary Logic** – utilizes each individual system's score output, mapped to a Operator-programmable symbolic formula to make the final decision. For example, the formula $((C \& N) | (B \& N)) | M$ would mean that in order for users to be verified, they would have to either pass Cross Match and Nuance, or Bioscrypt and Nuance, or Morpho. This decision methodology is most closely represented by System 3 in Modeling Multimodal Systems, above.
- **Weighted Decision** – This method utilizes an operator-specified multiplier (W_a , W_b , W_c , and/or W_d) along with system-level match results (A , B , C , and/or D). The weighted values are summed and averaged, then applied against an operator-defined global threshold to make the final decision. The formula for this method is $(A*W_a + B*W_b + C*W_c + D*W_d) / 4$. This decision methodology is most closely represented by System 4 in Modeling Multimodal Systems, above.

Unplayable Vocal Files. Nuance uses a special sound format for which the functions for playing back the recorded voice files are not included. IBG mitigated this condition by providing an external voice file player to enable DRDC to play back the recorded voice files. While this feature is not integrated into the fusion demonstration system, it provides the necessary functionality to overcome this inherent shortcoming.

Multiple Voice Signals. DRDC wanted to test the voice component of the fusion demonstration system with different voice base devices. However, there was no connection available that could input the signal into the PC directly. Thus, IBG developed a voice switch box with amplifier to enable DRDC to test the system with other voice base device, such as the radio and telephone. The system schematic is as follows:

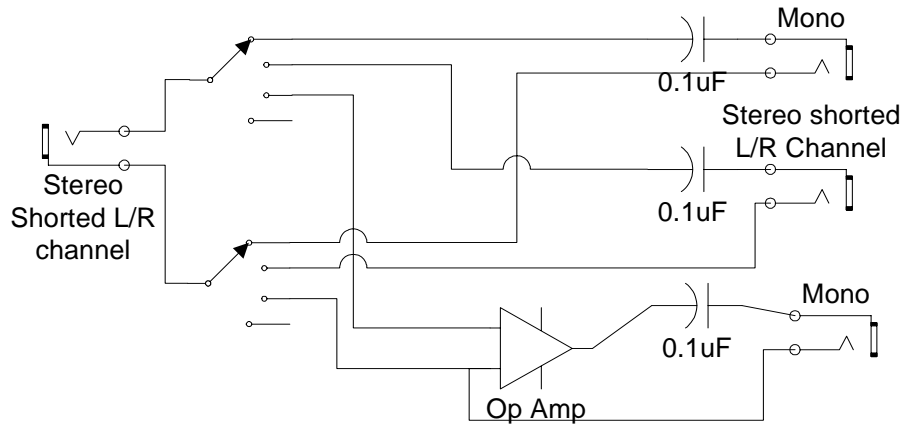


Figure 9. Voice Verification Input Schematic

4.2 BFDS Development Software and Hardware

IBG utilized the following development tools, SDK's, and hardware for the development of the BFDS.

Table 3. BFDS Development Toolkits and Software	
Operating System	Microsoft Window XP Professional Version 2002, SP1
Development Environment	Microsoft Visual C++ .NET 69586-335-0000007-18293
Voice Technology	Nuance Voice Platform 2.0 Nuance Speech Recognition System Version 8.5 Nuance Verifier Version 3.5
Optical System 1: Fingerprint Matching Algorithm/Device Driver	Cross Match USB SDK Toolkit Version 2.000
Optical System 2: Fingerprint Matching Algorithm/Device Driver	Sagem MorphoKey 3.3 with updated MSO driver for Dell video system
Silicon System: Fingerprint Matching Algorithm Device Driver	Bioscrypt SDK Core for ST Microelectronic - Version 5.0ST Microelectronics PerfectPrint PC API 8.3 (for Bioscrypt capture)

Table 4. BFDS Hardware	
PC	Dell OptiPlex SX2700, 2.8G Pentium 4, w/512 M RAM
Display	Mitsubishi 15" LCD monitor DiamondPoint V50LCD.
Silicon Fingerprint Device	ST Microelectronics fingerprint reader USB Model
Optical Fingerprint Device 1	Cross Match Verifier 300 USB model
Optical Fingerprint Device 2	Sagem Morpho Smart MSO 100 USB scanner

4.3 BFDS Applications

BFDS facilitates the requisite functions of data collection, cross comparison, and fusion authentication with customizable logic and score generation through the two following applications.

- **DRDC Enrollment: *Enrolment and Fusion*.** This application allows the operator to acquire enrolment and matching samples, select samples, perform biometric matching, and use a customizable fusion decision process with adjustable thresholds to compute a final decision.
- **DRDC Cross Comparison: *Large-Scale Matching*.** This application enables DRDC to perform the cross comparison of biometric samples to generate large quantities of scores, facilitating further quantitative analysis.

The following sections provide a more thorough explanation of each application. An Operator Manual for the applications can be found in Annex A.

4.3.1 DRDC Enrolment

Data Collection. The DRDC Enrollment application allows Operators to collect a User's biometric samples via one or more systems. The application allows the Operator to configure the number of samples to be collected and to determine from which finger (e.g. index, middle) to collect samples. For voice acquisition, the application enables the Operator to specify the number of voice samples to be collected. Once data collection starts, the application prompts the User to provide the specified biometric(s) via the specified device(s) until data collection requirements are satisfied.

The application requires Operator control over the collection process, providing considerable flexibility in the types of data that could be collected. The operator can assess the quality of the collected samples and avoid the inadvertent enrolment of unusable data into the system.

The Operator can also specify the target path location in which to store the raw sample, the reference biometric template, and the matching templates. Both the reference and matching templates can be automatically regenerated from the stored sample. Reference and matching templates are stored simply to accelerate the matching process.

Each fingerprint collected is stored in the sample directory. This directory structure can be customized in several ways. Unique sets of data, such as those for good quality prints, incomplete prints, and bad quality prints, can be stored in different sample sets. Under varying test scenarios, the operator could merge different sets of data into a single testing directory. Furthermore, this directory structure allows the operator to separate random or demonstration test samples from the main data sets.

Filename Structure. Each collected biometric sample will create up to three unique files for the raw sample, reference template (optional), and matching template (optional). The filename's extensions may differ based on the modality, but the base filename structure is the same. The filename is structured as [Subject ID]-[Biometric Feature]-[Sequence], with the following data elements:

Table 5. BFDS Filename Data Elements											
Subject ID	Operator-entered ID associated with a specific individual for data collection										
Biometric Feature	<p>0= unknown (voice)</p> <table> <tr> <td>1 = right thumb</td><td>6= left thumb</td></tr> <tr> <td>2 = right index</td><td>7 = left index</td></tr> <tr> <td>3=right middle</td><td>8= left middle</td></tr> <tr> <td>4=right ring</td><td>9= left ring</td></tr> <tr> <td>5=right little</td><td>10= left little</td></tr> </table>	1 = right thumb	6= left thumb	2 = right index	7 = left index	3=right middle	8= left middle	4=right ring	9= left ring	5=right little	10= left little
1 = right thumb	6= left thumb										
2 = right index	7 = left index										
3=right middle	8= left middle										
4=right ring	9= left ring										
5=right little	10= left little										
Sequence	Incremental number representing the sequence in which the print was collected (sequence=1 for single-acquisition configuration).										

Directory Structure. The Operator can configure the base directory from the main dialog box for storage of raw samples, reference templates, and matching templates. This procedure is addressed in Annex A. The application creates unique directories for each system. By default, fingerprint images are saved as .BMP files, and voiceprints are saved as .WAV files. Nuance files are saved in a proprietary .WAV format that requires Nuance-specific tools for playback.

The Cross Comparison and Fusion functions operate based on these filename and directory structures. The operator can execute various test cases by pointing the applications to different directories.

Fusion Demo. This application component provides a dialog box indicating a Subject ID for matching. The decisions of the outcome are based on the fusion methods described under 4.1.3.

To start the fusion test, the Operator selects a subject ID to match against. If necessary, the operator can also select the specific set of prints (e.g., Cross Match right index finger). Once the subject ID is selected, the Operator captures the requisite biometric samples. After the sample collection is completed, the program displays match results in terms of false non-match rate (FNMR) and false match rate (FMR) in the right-hand window. The Operator can re-evaluate results with different IDs or decision criteria configurations, and change fusion weighting and decision parameters by selecting “Config...” and utilizing the sub-menu. The program will then re-evaluate and display the results with the newly selected reference and/or fusion parameters.

4.3.2 Cross Comparison

This application allows the operator to select a system for which cross comparison of all genuine and impostor datasets will be executed. Once a system is selected and the process executed, the application matches a User’s data against all existing prints (fingerprint or voice) stored in that system. The cross comparison function performs an $N*(N-1)$ match, where the tested print is matched against all the selected prints (minus itself).

The match result is saved in the specified directory as a Comma Separated Variable (CSV) file. The following is a sample of the .CSV output format:

"Vendor","Ref-file","Ref-ID","Ref-Feature","Ref-Num","Mat-file","Mat-ID","Mat-Feature","Mat-Num","Score"

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-007, 003, 07, 007, 69.0594

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-006, 003, 07, 006, 68.8028

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-005, 003, 07, 005, 58.0065

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-004, 003, 07, 004, 64.9340

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-003, 003, 07, 003, 58.9433

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-002, 003, 07, 002, 63.9873

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-001, 003, 07, 001, 65.5554

Bioscrypt, 003-07-008, 003, 07, 008, 003-07-000, 003, 07, 000, 65.2465

Bioscrypt, 003-07-008, 003, 07, 008, 003-02-008, 003, 02, 008, 13.7068

Figure 10. Sample Cross Comparison .CSV Output

The following table encapsulates the descriptions for each field and value.

Table 6. Field Descriptions for cross comparison output files			
Vendor	Vendor of the technology for this comparison		
Ref-File	Base reference filename for this match row		
Ref-ID	Reference subject ID number		
Ref-Feature	Biometric feature:		
	0= unknown (voice)		
	1 = right thumb	6= left thumb	
	2 = right index	7 = left index	
	3=right middle	8= left middle	
	4=right ring	9= left ring	
	5=right little	10= left little	
Ref-Num	Reference sequence number		
Mat-File	Base matching filename for this match row		
Mat-ID	Matching subject ID number		
Mat-Feature	Matching feature type (see ref-Feature for feature code)		
Mat-Num	Matching sequence number		
Score	Match result score 0.0 – 100.0		

5. Potential Enhancements to Military Applications

5.1 General Advantages of Multimodal Biometric Systems

Multimodal biometric systems are designed to provide the following general benefits over individual, monomodal biometric technologies:

- Reducing false non-match rates and false match rates. By deploying more than one biometric technology for 1:N and/or 1:1 processing, and intelligently combining or fusing match results from both systems, it is possible to reduce the overall system's matching error rates. For example, to reduce 1:1 false matching, a multimodal system can provide two subsystems against which a user must match in order to defeat the system. Similarly, to reduce 1:1 false non-matching, a multimodal system may only require that a user match against one of two subsystems.
- Providing a secondary means of enrolment, verification, and identification for users unable to enroll and/or authenticate through a primary biometric technology. By deploying more than one biometric technology, a deployer can ensure that a higher percentage of individuals are enrolled and matched in a biometric system, reducing the need for fallback or secondary processing. This in turn can reduce costs and security risks.
- Combating attempts to spoof biometric systems through non-live data sources such as fake fingers. By implementing a multimodal system that requires dual authentication, an attacker must successfully spoof both systems, or spoof one while attempting to match as an imposter in another.

These direct benefits can lead to indirect benefits such as increased system security, reduced deployment costs, and increased ease of use. However, realizing benefits from a multimodal biometric system requires intelligent combination and utilization of technologies, devices, and algorithms; requires an application for which a multimodal solution is both viable and useful; and requires effective design of enrolment and matching processes. In military applications, multimodal fusion biometrics could be implemented to address a wide range of authentication issues, for both physical and logical access to secured facilities and information, as well as enhancements to field operations.

5.2 Multimodal Biometrics in Military Applications

A multimodal fusion biometric system can be harnessed to authenticate authorized users for access to high-security facilities and to classified or sensitive information. These security applications could potentially be fused into a single system, as an authorized user's biometric score for physically entering a room could be fused with the results of a fingerprint verification for access to a PC desktop or network. Alternatively, a pre-condition for even attempting to log into a PC may be a simple yes/no decision indicating whether the same person had entered the room in the first place. In doing so, the system not only authenticates whether the user is permitted to use the computer, but also records whether the user entered the room where the PC is housed prior to the authentication attempt. This could deter instances of "piggybacking," whereas a person immediately follows an authorized person through the door and attempts to access the resources housed in the room. The strong security and auditing capabilities of biometrics can be combined to track a single user's entire path from entering the main door to a facility to accessing specific computers and files. The potential number of combinations in biometric technologies and the concomitant deployment options for military applications are considerable.

Access to Classified or Sensitive Information. Biometrics can be used to identify or verify the identity of individuals accessing workstations, servers, networks, laptops, and other PC-oriented resources, as well as PDAs and handheld computing devices. The biometric is used to complement or replace authentication mechanisms such as passwords and tokens, which are susceptible to theft or sharing. In an environment where every authorized user must access PC's or networks for retrieving sensitive or classified information, a multimodal biometric system mitigates the problem that all biometric technologies face with regard to enrollment. Having the ability to verify multiple biometric features ensures that almost all of the authorized users will have some means of authenticating onto a system, whether through their fingerprint, iris, or facial features. From a purely security-oriented perspective, a multimodal biometric system in conjunction with existing procedures, such as passwords and tokens, provides a multi-factor authentication paradigm that is difficult to bypass through forgery or spoofing. A fusion decision methodology has the flexibility to provide the optimal balance in authentication between maintaining a higher level of security and minimizing false rejections for specific applications.

Physical Access to Secured Facilities. Biometrics can be implemented to identify or verify the identity of individuals entering or leaving an area, typically a building or room, at a given time. The biometric is used to complement or replace authentication mechanisms such as keys, tokens, and badges. This application of biometrics is highly relevant to the military, as most installations and facilities require some level of authorization for physical access. Furthermore, certain floors and rooms may require access by individuals with a higher level of security clearance than others within the same building, which necessitates access control measures beyond just the main entrance to the facility. Multimodal biometrics can be harnessed to facilitate this level

of complex physical security for multiple locations without the added cost of hiring more security personnel

Enhancement to Field Operations. Verifying the identity of soldiers out in the field before communicating secure information is an area in which a multimodal biometric solution may be well-suited. For example, personnel requesting access to sensitive or classified information from a remote site may be able to verify their identity by presenting multiple biometric samples. A useful analogue in the commercial world comes from a biometric website access solution, where the system automatically dials the registered person's phone number to verify their voice once the person logs into the web site to execute a secured transaction. Similarly, a multimodal biometric system for military use could be set up to dynamically request a voiceprint, in conjunction with a fingerprint verification that matches on the device, when personnel attempt to remotely access restricted information. The time elapsed in performing such a verification may be prohibitive for certain applications, thus this implementation may be limited to high-security transactions where time is not a critical factor.

Device/Weapons Access. In the near future, multi-factor authentication could be implemented to facilitate device and weapons access for military use. For using communication devices, the user may need to verify their fingerprint on a small, silicon platen that matches on the device and then authenticates the user's voice over a centralized, secure server. Weapons access could include authentication for activating individual weapons, for opening a storage bin housing several weapons, or for activating military equipment (such as tanks) via multifactor verification. There are several major challenges in implementing such a system for weapons access. First, the ramifications of a false rejection could potentially be fatal, thus there is a heightened need for a multimodal biometric solution. However, verifying multiple biometric features increases the time elapsed during the transaction, which is particularly disadvantageous in applications that require extremely quick action.

Case Study: US Military and Intelligence Biometrics Automated Toolset (BAT)³. United States officials announced in January 2002 that U.S. military and intelligence operatives were using the Biometrics Automated Toolset (BAT) to create digital biometric files of terrorism suspects detained in Afghanistan and in Guantanamo Bay. This data collection effort encompassed iris, fingerprint, face and voice technologies. Led by Northrop Grumman, the BAT was developed in the Army Battle Lab at Fort Huachuca, and incorporated Viisage (face), Cross Match (finger), and Iridian (iris) technologies.

The BAT system consists of approximately 450 laptops equipped with multiple biometric capturing devices, 400 of which were specially prepared for the Iraq invasion of 2003. To supplement the collection of biometric data, surveillance photos and fingerprints gathered from confiscated objects are included in the dossiers. In addition to biometric data, dossiers also contain text from prisoner interrogations, video or sound clips, and digital images of items seized during a search. All dossiers

³ Krane, Jim. Biometrics: U.S. Building Terror Dossier, October 10, 2002.
www.sltrib.com/2002/Oct/10302002/business/11836.htm

are stored in a central database at a U.S. intelligence agency. The primary benefit of the central database, which includes a range of non-biometric intelligence information, is that it overcomes historical secrecy barriers, providing border officials and police departments with a straightforward and relatively rapid search mechanism to determine if the individual is a terrorism suspect without revealing sensitive intelligence. An additional benefit is that the database can be searched from remote locations via a satellite telephone.

Presently, BAT files have been shared with the FBI and the Immigration and Naturalization Service. The INS has incorporated BAT into the search system of practically all U.S. entry points, Border Patrol stations and INS field offices. Furthermore, in May of 2002, a bill was introduced to the Senate that would require the CIA to create a database of known or suspected terrorists that could be accessed by federal, state, local and foreign governments.

5.3 Challenges Facing Multimodal Systems

Potential multimodal deployers must determine whether improvements in accuracy, enrollment levels, and anti-spoofing capabilities sufficiently offset potential increases in acquisition and processing time, user and operator effort, deployment expense, systems integration effort, and added points of failure. Major challenges facing multimodal system development and implementation include the following:

- **Impact on Current Processes.** With the exception perhaps of facial and iris recognition, every multimodal technology combination required more time and effort on the part of the end user. Such process impact is more problematic in transactional verification than in initial enrollment; however, requiring extensive effort in any environment will dramatically reduce system effectiveness.
- **Standardization and Interoperability.** While standards for monomodal systems are emerging and becoming adopted, few standards address any element of multimodal systems, including design, data formats, performance, or systems interfaces. Deployers risk implementing proprietary systems in lieu of such standards.
- **Costs.** Multimodal systems bear increased costs in terms of acquisition devices, matching systems, and user and operator training. Such costs may be offset by commensurate reductions in manual processing.
- **Training and Acclimation.** In transactional multimodal systems, users must be trained effectively on each biometric system involved. In addition, users must remain familiar with the methods of interacting with each device, or error rates are likely to increase.
- **Security Challenges.** Multimodal systems can introduce divergent security risks. First, the biometric system has more points of failure, such that communications and data storage methods must be examined with care. In addition, system operators may be prone to reverting to fallback or secondary biometric processing

too quickly, such that the benefits of placing a stronger biometric technology first are lost.

6. Recommendations for Future Work

6.1 Technological Recommendations

DRDC Ottawa may benefit from expanding the BFDS functionality. While the current demo system provides the requisite functions and flexibility to gain a robust understanding of multimodal technologies and fusion techniques, expanding the system's capabilities would enable DRDC to more comprehensively study fusion methods and to explore the viability of potential applications. BFDS expansion can be explored as follows:

Adding Biometric Systems and Modalities. DRDC may consider integrating a wider variety of biometric devices and modalities within BFDS. The current platform can be expanded to incorporate 1:N solutions designed to search databases, an application of general interest to military planners (as evidenced by the US military's BAT system). Adding iris and facial recognition components to BFDS would considerably expand the system's capabilities and provide broader parameters for experimentation. As practical applications may rely on technologies beyond fingerprint and voice verification, DRDC would benefit through further testing of various modalities in a fusion environment.

Enhancing Cross Comparison Testing Capabilities. While the BFDS currently enables cross comparison testing of biometric samples within a given technology, it does not enable cross-sensor and cross-algorithm testing. Testing fingerprint images acquired through one device against multiple algorithms, for example, can provide insights into a system's multi-algorithm capabilities. This added functionality would greatly expand the types of cross comparison tests at DRDC's disposal. A large-scale deployment of a multimodal biometric system may require the implementation of several technologies, such that studying the performance of the underlying algorithms across multiple capture platforms would generate a considerable amount of useful data for DRDC. IBG's Comparative Biometric Testing may be able to play a role in supporting or enhancing such an initiative.

6.2 Strategic Recommendations

While DRDC is currently exploring biometrics for the purpose of conducting scientific tests of the technology, the eventual objective is to define contexts in which multimodal fusion biometrics could be deployed in practical, real-world military applications. The cutting-edge nature of this work, along with the major biometric initiatives underway across the Canadian government, could position DRDC in a leadership role in defining system requirements, compatibility standards, and performance specifications. In light of these considerations, IBG recommends the following actions:

Piloting Specific Applications. DRDC may consider piloting multimodal biometrics in practical military applications. The number of potential biometric applications for this environment is considerable, and the nature of multimodal systems is such that several of these applications could be tied into one pilot system. DRDC could conceivably build a demo room in which an expanded BFDS could control access to a door as well as to a PC inside the room. In addition to authenticating at the door and while logging onto the PC, the pilot could be set up so that the user verifies against a third biometric system in order to gain access onto the internal network. Verification of individuals for remote information access could also be tied into this pilot, demonstrating a wide-range of applications for various usage scenarios. Such a pilot would generate a considerable amount of useful, real-world test data. It would also establish DRDC as one of the leading authorities in multimodal biometric systems from both a scientific and application perspective. IBG's extensive experience in executing feasibility assessments, designing pilots, and formulating pilot evaluation metrics provides DRDC with the resources for successfully running both small and large-scale pilots.

Establishing a Biometric Centre of Excellence. The primary opportunity for DRDC to position itself as the hub of all things biometric in the Canadian government is in the conception, establishment and ongoing operation of a Biometric Centre of Excellence. This Biometric Centre of Excellence (CoE) would have as its primary goal to provide ongoing testing, validation, training, research, and conformance and compliance certification in the area of biometric technologies and systems, as well as showcasing biometric applications. The CoE is not necessarily seen as a single facility; it may be a network of facilities, potentially co-located with existing commercial or academic institutions, working under DRDC's central direction. The establishment and continued operation of such a centre would position DRDC as the biometric authority within the Canadian government.

Annex A: BFDS Operator Manual

BFDS Login

After logging into Windows on the BFDS PC, the following screen appears.

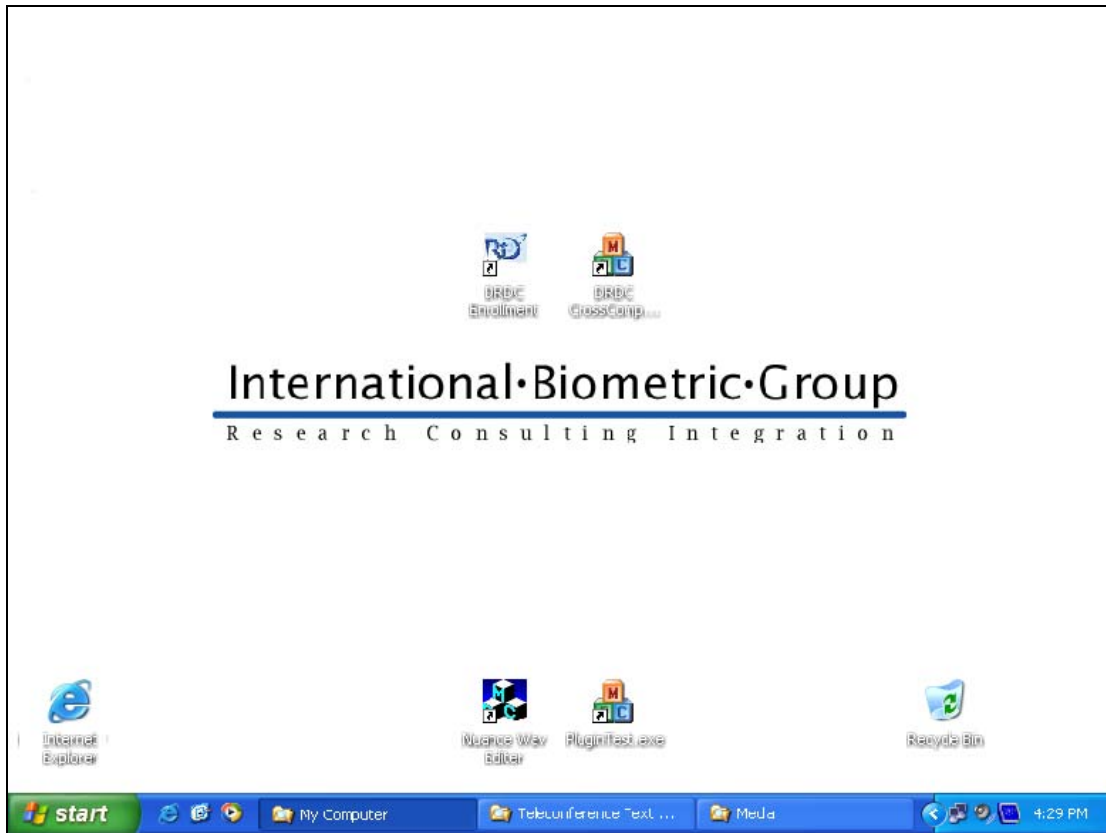






Figure 11. Application Icons

BFDS Applications

Four executables are associated with the BFDS application. DRDC Enrollment – for data collection and Fusion demonstration and 2) DRDC Cross Comparison that generate the raw matching data

Table 7. Application Description	
	DRDC Enrollment Primary data collection and fusion demonstration program Location: C:\DRDC Fusion\ directory
	DRDC Cross Comparison Provides cross-comparison functionality for stored data, generates scores in CSV format Location: C:\DRDC Fusion\ directory
	Nuance Wav Editor Nuance sound file player and editor used to edit Nuance .wav files C:\Nuance\V8.5.0\Win32
	PluginTest Sample Plug-in test tool for DRDC to test its own Plug-ins Location: C:\DRDC Fusion\ directory

MAIN INTERFACE

FUSION GENERATION

REVIEW, ADD TO EXISTING ENROLLMENT

ENROLL NEW USERS

SELECT CONFIGURATION MODE

CONFIGURE ENROLLMENT PARAMETERS

CONFIGURE FUSION PARAMETERS

Figure 12. Operator Interface Map

Main Enrollment Screen

After starting **DRDC Enrollment**, the Operator can (1) review a previous enrollment by selecting a Subject ID from the Subject ID Drop-Down or (2) enter a new Subject ID to acquire biometric data from a new User.

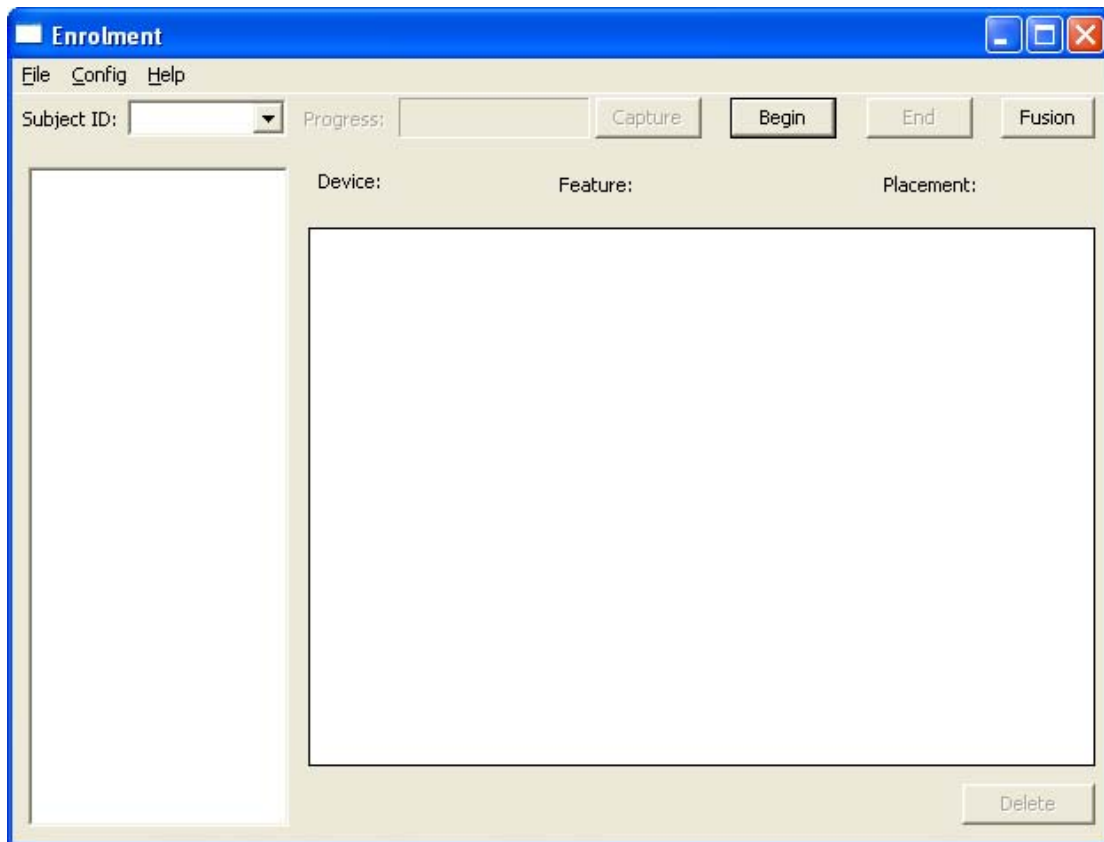


Figure 13. Main Enrollment Screen

Enroll New Users

To acquire data from a new User, the Operator enters an unused number in the Subject ID box. The Operator selects “Begin”. The User is prompted to present the specified biometric characteristic (e.g. left index) to the specified device (e.g. Sagem MORPHO). Data collection follows the current enrollment parameter configuration. Multiple samples are generally acquired for each biometric characteristic in order to determine the degree to which repeated fingerprints or voice patterns vary.

The process differs slightly for fingerprint and voice. For fingerprint, once the biometric is presented, the Operator selects “Capture” to acquire the biometric sample. For voice, the Operator selects “Capture”, and the User states the specified password or passphrase.

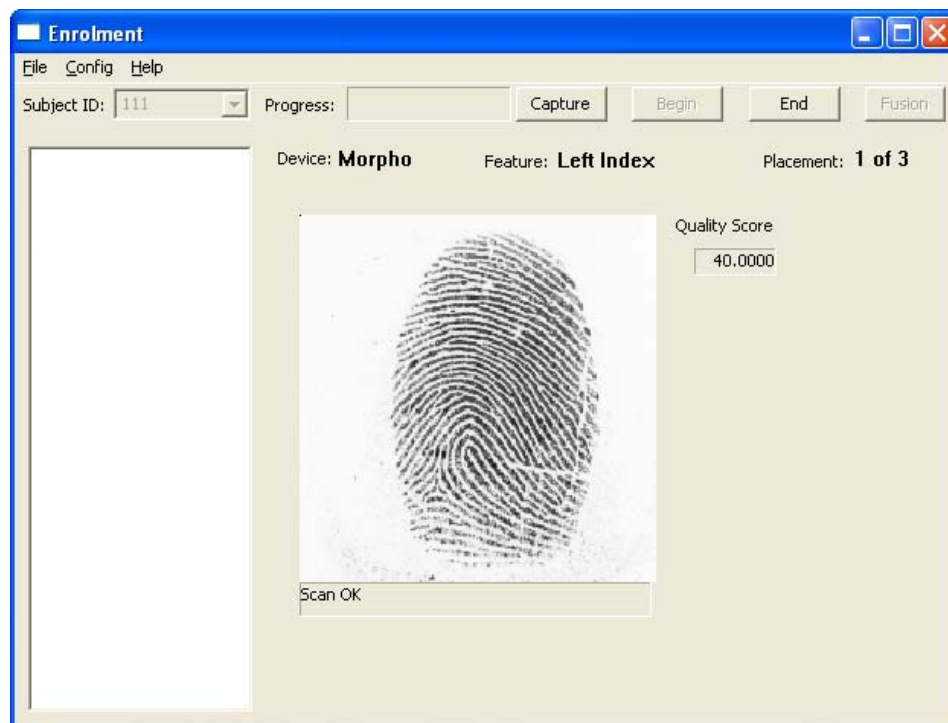


Figure 14. Capture Interface

Note that the Quality Score to the right of the fingerprint image is a vendor-specific measure of the usability of the fingerprints for ongoing matching. It may be of interest to the Operator to collect images with intentionally low quality scores.

Review and Add to Existing Enrollments

To view biometric data associated with an existing User, or to add new biometric data to an existing Subject ID, click on the down arrow [003] and select an enrolled User. Once a valid ID is selected, all available samples associated with that User are listed on the left of the GUI. Once selected, fingerprint samples presented as .bmp images appear on the right of the GUI. Voice samples in the left-hand list must be double-clicked to be played.

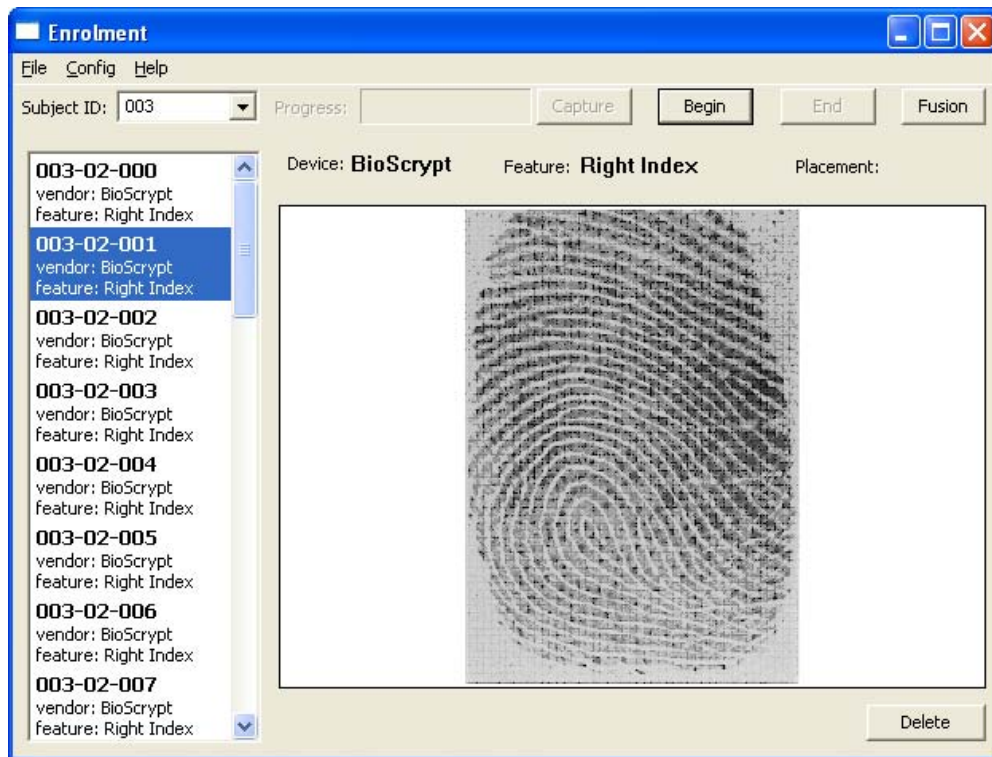


Figure 15. Reviewing Previous Enrollments

Nuance's voice file format is not supported by Microsoft's Multimedia format. Nuance's player must be used to activate the voice file.

Adding biometric to existing subject

To collect additional biometric samples for an existing User, select "Begin" to start data collection. Data collection follows the current enrollment parameter configuration.

Enrollment Configuration

User enrollment can be configured by the Operator. BFDS can collect one or more samples from one or more characteristics, and can enable 1-4 systems.

Samples per feature controls the number of fingerprints acquired from each finger, e.g. left index, as well as the number of voice samples acquired. The tick-boxes for the ten fingers control which of the fingerprints are sampled (voice is automatically sampled if Nuance is selected). The Plugins tick-boxes control which biometric systems are used for enrollment and matching.

Configure Enrolment

Folders

Samples: c:\Projects\Drdc\build\debug\Repository\samples

Reference Templates: c:\Projects\Drdc\build\debug\Repository\reference

Match Templates: c:\Projects\Drdc\build\debug\Repository\match

Capture

Samples per feature: 3

Biometrics:

Fingerprints	
Left Hand	Right Hand
<input type="checkbox"/> Thumb	<input type="checkbox"/> Thumb
<input checked="" type="checkbox"/> Index	<input checked="" type="checkbox"/> Index
<input type="checkbox"/> Middle	<input type="checkbox"/> Middle
<input type="checkbox"/> Ring	<input type="checkbox"/> Ring
<input type="checkbox"/> Little	<input type="checkbox"/> Little

Plugins:

- ☒ Bioscrypt-ST Micro Plug In --Fingerprint
- ☒ CrossMatch Plug In --Fingerprint
- ☒ Nuance Plug In --Voice
- ☒ SAGEM Morpho Plug In --Fingerprint

OK Cancel

Figure 16. Enrollment Configuration

In the Figure above, three samples will be acquired from each of the left and right index fingers for each fingerprint system in addition to three samples for the voice system. Biometric data in sample and processed template form is stored in the directories as indicated in the figure. Reference and match templates are generated from samples, and are used by certain systems to effect biometric matching. If one or more templates are missing or are older than a newly acquired sample, BFDS automatically generates the template from the sample.

Fusion-Based Matching

In order to match against enrolled data and to perform various fusion experiments, the Operator selects “Fusion” from the Main Enrollment screen. The Operator then selects a User against whom to test. The left hand side of the GUI presents the Plus-Ins, or biometric systems, in which the User is enrolled.

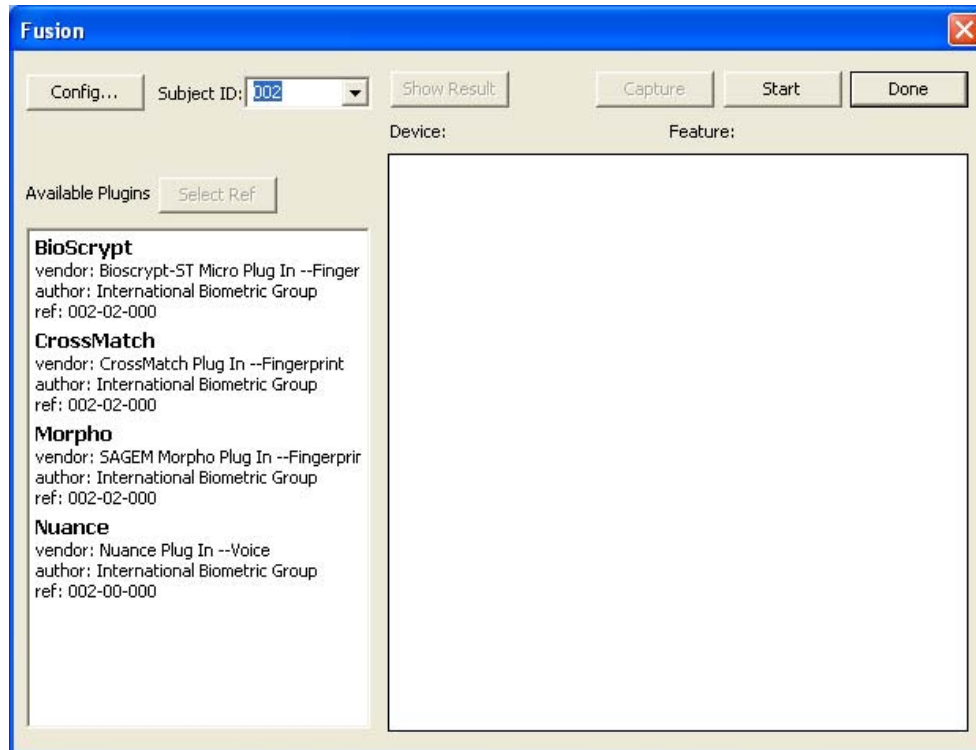


Figure 17. Fusion-Based Matching Interface

By default, the application is designed to match against the last collected sample. The Operator may select a different sample by selecting the Vendor Plug-in then selecting “Select Ref”. A dialog box shows all available biometric samples for selected User. The Operator can select the samples against which to match then select “OK”.

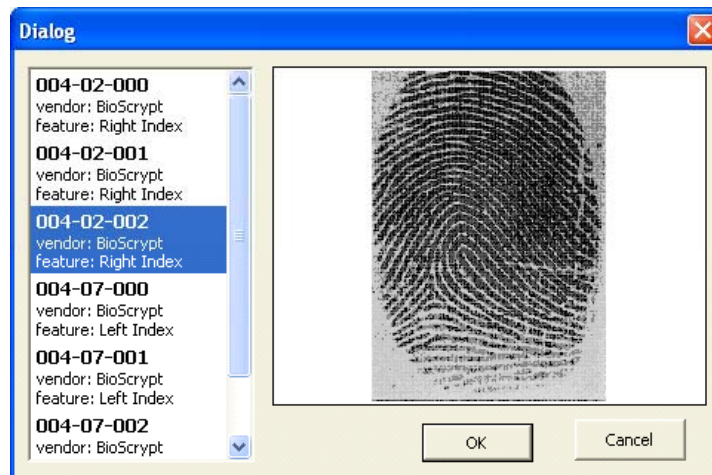


Figure 18. Selecting Samples for Fusion Matching

Collecting Live Samples

The Operator selects “Start” to acquire a match sample to be compared against enrolled samples, generating system-specific scores and subsequent fusion scores. Match samples are acquired for each system in which the User is enrolled. The match sample is erased once the test is completed.

Fingerprint systems show a live sample from the scanner. The Operator must click “Capture” to acquire the sample. Voice systems require that the Operator select “Capture”, at which point the User speaks into the microphone or other collection device.



Figure 19. Live Acquisition Interfaces: Fingerprint and Voice

Fusion Results and Experiment Mode

Once the match sample(s) are collected, they are matched against the enrolled samples and the following report is generated.

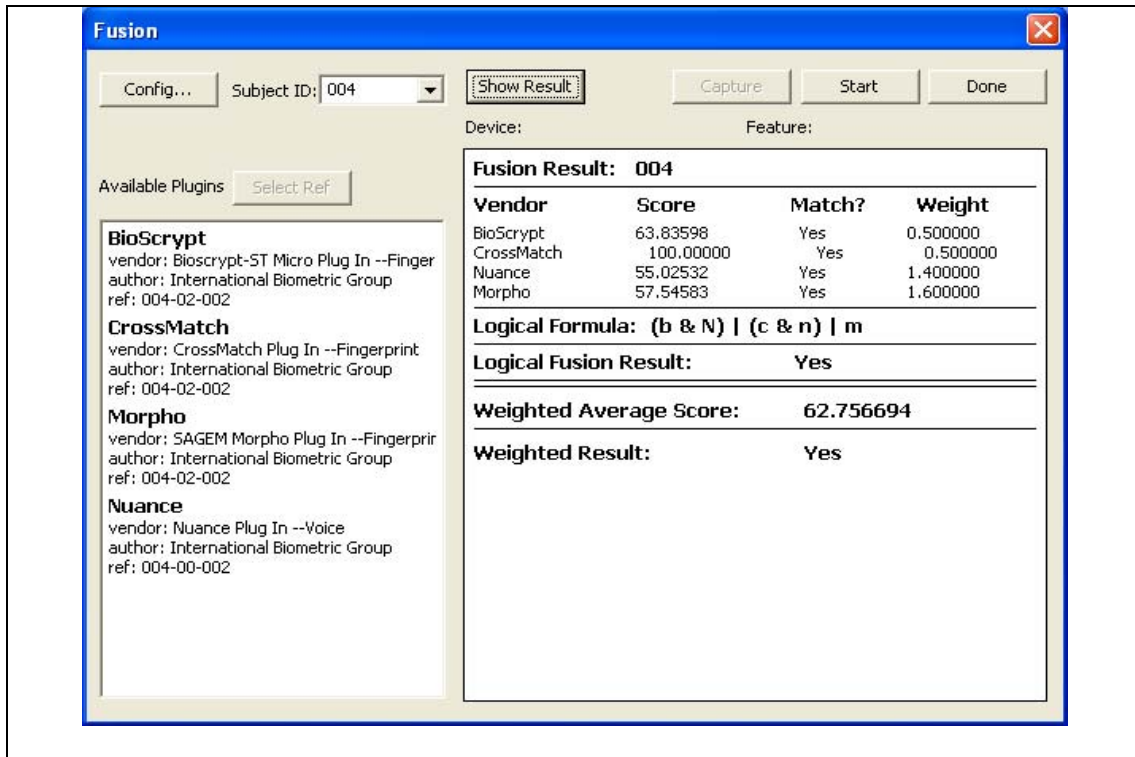


Figure 20. Fusion Output Interface

This Figure indicates the fusion results for a user enrolled in all four biometric systems.

- **Vendor:** indicates which system generated the score
- **Score:** the normalized score output
- **Match?:** a Yes/No decision associated with a specific system
- **Weight:** the relative importance of a biometric system's score in an overall fusion decision, with 1 as a baseline
- **Logical Formula:** and/or fusion logic based on non-weighted vendor scores
- **Logical Fusion Result:** Yes/No output resulting from Logical Formula
- **Weighted Average Score:** score result based on averaging of weighted vendor scores
- **Weighted Result:** Yes/No output resulting from Weighted Average Score vs. cumulative threshold

The Operator can experiment with “what if” cases. For example, the Operator can select a new User or a different biometric characteristic against which to execute matching. The Operator can also alter Fusion configuration parameters (described below) by selecting “Config...”, changing parameters of interest, and selecting “Show Result”.

Fusion Configuration

The following dialog illustrates the various ways in which BFDS enabled management of thresholds, fusion logic, and weighting.

1. Operator-adjustable “**Threshold**” settings are established for each system, based on normalized vendor match thresholds.
2. Operator-adjustable “**Logical Formula**” settings enable symbolic logic strings used for “and/or” fusion, based on Users’ ability to exceed the thresholds above.
3. Operator-adjustable “**Weighted Fusion**” enables different systems to assume larger or smaller roles in the overall matching logic. Systems B, C, M, and N can be assigned values greater or less than 1.0 to increase or reduce, respectively, the degree to which each informs overall matching logic.
4. System scores, multiplied by their respective fusion weights, are averaged and compared to a “**Weighted Fusion Threshold**”, generating a global fusion score. In the Figure below the global threshold is 50.

The image shows a Windows-style dialog box titled "Fusion Config". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into three main sections: "Variables and Operators", "Logical Fusion", and "Weighted Fusion".

- Variables and Operators:** This section contains a text field with the string "B:Bioscript; C:CrossMatch; M:Morpho N:Nuance; &:And |:Or".
- Logical Fusion:** This section contains a "Thresholds:" label followed by four input fields: B (35), C (70), M (8.3), and N (50). Below these is a "Formula:" label followed by a text field containing "b|c|m|n" and a "Syntax Check" button.
- Weighted Fusion:** This section contains a "Weight:" label followed by four input fields: B (1), C (1), M (1), and N (1). Below these is a "Threshold" label followed by an input field containing "50".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 21. Fusion Configuration Interface

To illustrate a logical formula, if an Operator hypothesized that a MORPHO match were sufficient to constitute an overall match, but that non-MORPHO systems also needed a match on a voice system, the following would be utilized:

$(B \ \& \ N) \ | \ (C \ \& \ N) \ | \ M$

The User would be match if (1) Bioscript and Nuance, (2) Cross Match and Nuance, or (3) Morpho were successful matches.

Cross Comparison

This program allows Operators to compare all samples on file for each vendor, generating a Comma Separated Value (CSV) file with system-specific scores. The Operator selects the system of interest in the left panel; the right panel indicates the number of samples available and the total comparisons to be executed (genuine and impostor). To execute cross-comparative matching, the Operator selects “Start”. This button toggles to “Stop”, allowing the Operator decides to stop a lengthy cross-comparison.

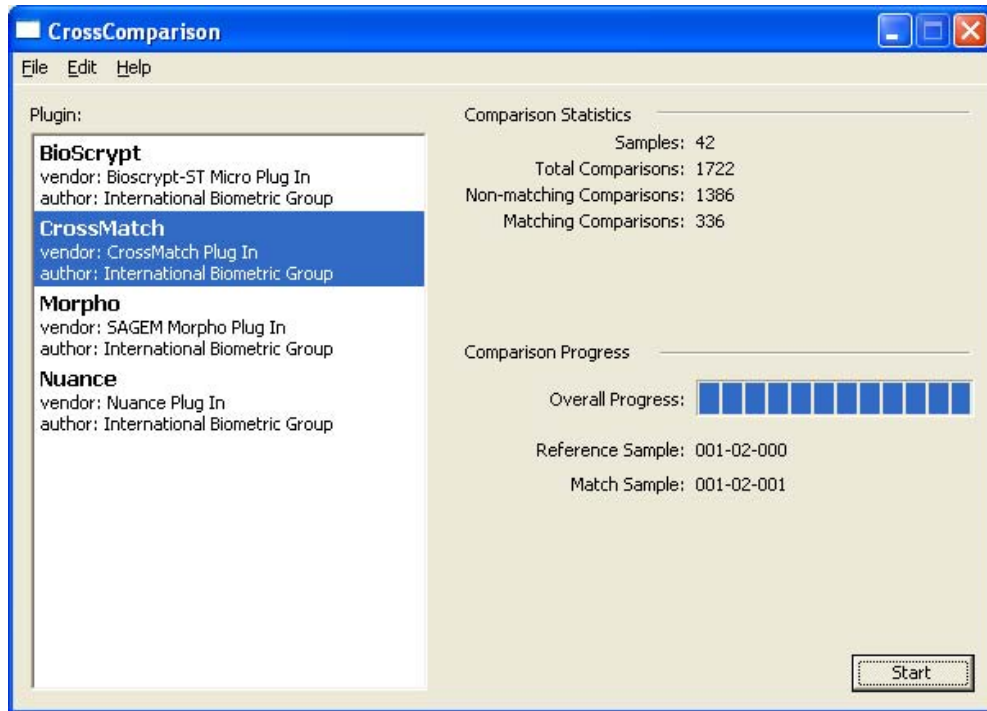


Figure 22. Cross Comparison Interface

The result CSV file is saved in the folder specified in the Cross Comparison Configuration’s “Comparison Output” dialog box. The filename is vendornamematchsequence.csv, e.g. bioscript02.CSV.

Cross Comparison configuration

Operators can specify the root folder location for samples, reference templates, match templates and CSV outputs.

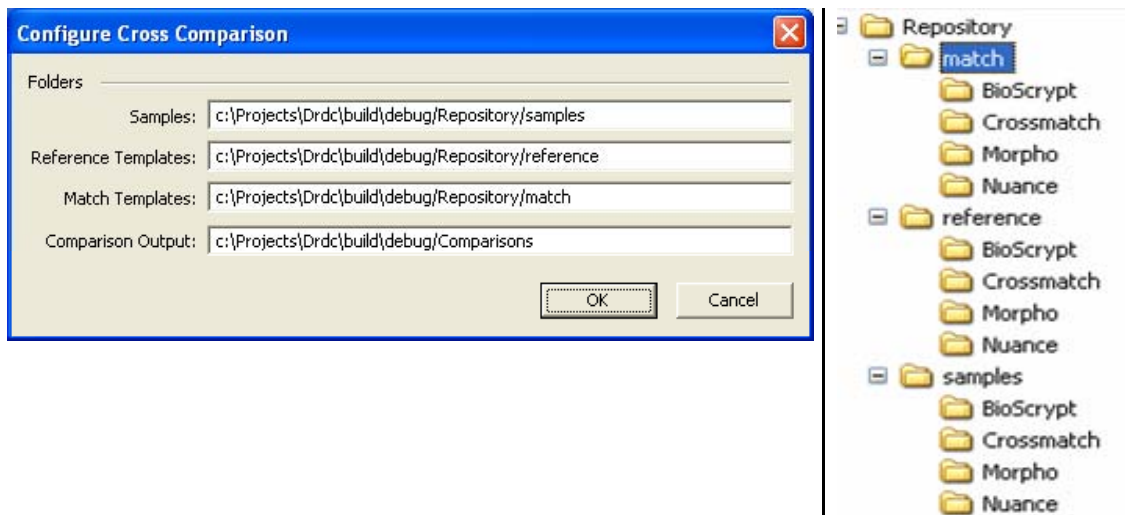


Figure 23. Cross Comparison Configuration

List of symbols/abbreviations/acronyms/initialisms

AFIS	Automated Fingerprint Identification System
BFDS	Biometric Fusion Demonstration System
CCD	Charged-Couple Device
CMOS	Complementary Metal Oxide Semiconductor
DND	Department of National Defence
FMR	False Match Rate
FNMR	False Non-Match Rate
FTA	Failure to Acquire
FTE	Failure to Enroll
OEM	Original Equipment Manufacturer
SDK	Software Development Kit

Glossary

Technical term	Explanation of term
FMR	The anticipated proportion of users able to match against another individual's enrollment in a biometric system
False Non-Match Rate	The anticipated proportion of users unable to match against their own enrollment in a biometric system
FTA	The inability on the part of a biometric system to record a sample from a user, often based on low-quality biometric data
Failure to Enroll	The inability on the part of a biometric system to acquire sufficiently stable and distinctive data to comprise an enrollment for a given user
Fusion	The use of multiple data sources and/or match outputs to execute biometric decisions, including but not limited to enrollment and matching
Multi-System	A biometric system comprised of more than one device and/or algorithm from within the same modality, e.g. two fingerprint systems
Multi-Modal	A biometric system comprised of more than one modality, e.g. fingerprint and face or face, voice, and iris

DOCUMENT CONTROL DATA		
(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)		
1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) International Biometric Group One Battery Park Plaza Ground Floor New York, NY 10004	2. SECURITY CLASSIFICATION (overall security classification of the document including special warning terms if applicable). UNCLASSIFIED	
3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C,R or U) in parentheses after the title). Biometric Fusion Demonstration System Scientific Report		
4. AUTHORS (Last name, first name, middle initial. If military, show rank, e.g. Doe, Maj. John E.) Mak, Mcken ; Kim, Joseph ; Thieme, Michael		
5. DATE OF PUBLICATION (month and year of publication of document) March 2004	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc). 71	6b. NO. OF REFS (total cited in document) 0
7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered). Contractor Report		
8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include address). DEFENCE R&D CANADA - OTTAWA 3701 Carling Avenue, Ottawa, Ontario, K1A0Z4		
9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Specify whether project or grant). 15BF27	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written). W7714-030754	
10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique.) DRDC Ottawa CR 2004-056	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor.)	
11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification) (X) Unlimited distribution () Defence departments and defence contractors; further distribution only as approved () Defence departments and Canadian defence contractors; further distribution only as approved () Government departments and agencies; further distribution only as approved () Defence departments; further distribution only as approved () Other (please specify):		
12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution beyond the audience specified in (11) is possible, a wider announcement audience may be selected).		

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

DRDC-Ottawa contracted International Biometric Group (IBG) to develop a biometric fusion application, utilizing three distinct fingerprint systems and one voice verification system. This application enables biometric data collection and sample matching as well as operator configuration of multi-system matching logic. The application provides sufficient data for DRDC to perform a range of quantitative analysis on the utility of biometric systems that use multiple systems within a given modality and multiple systems within multiple modalities. This document provides background information on the biometric technologies implemented within this demonstration application (fingerprint and voice verification). It describes various multimodal biometric concepts of operation for both verification and identification systems. It details the functionality accessible through the biometric fusions application. Lastly it provides an Operator manual for the application.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title).

Multimodal Biometrics, Biometric Fusion, Fingerprint Recognition, Voice Verification, Matching, Cross Comparison.